User Manual

DIR-853

AC1300 MU-MIMO Wi-Fi Gigabit Router with 3G/LTE Support and USB Port 3.0

March 2018

Contents

CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the router DIR-853 and explains how to configure and operate it.

This manual is intended for users familiar with basic networking concepts, who create an in-home local area network, and system administrators, who install and configure networks in offices.

Conventions

Example	Description
text	The body text of the manual.
Before You Begin	A reference to a chapter or section of this manual.
"Quick Installation Guide"	A reference to a document.
Change	A name of a menu, menu item, control (field, checkbox, drop-down list, button, etc.).
`192.168.0.1`	Data that you should enter in the specified field.
! Information	An important note.

Document Structure

Chapter 1 describes the purpose and structure of the document.

Chapter 2 gives an overview of the router's hardware and software features, describes its appearance and the package contents.

Chapter 3 explains how to install the router DIR-853 and configure a PC in order to access its web-based interface.

Chapter 4 describes all pages of the web-based interface in detail.

Chapter 5 includes safety instructions and tips for networking.

Chapter 6 introduces abbreviations and acronyms used in this manual.

CHAPTER 2. OVERVIEW

General Information

The DIR-853 device is a wireless dual band gigabit router with 3G/LTE support. It provides a fast and simple way to create a wireless and wired network at home or in an office.

The router is equipped with a USB port for connecting a USB modem[1], which can be used to establish connection to the Internet. In addition, to the USB port of the router you can connect a USB storage device, which will be used as a network drive, or a printer.

Also you are able to connect the wireless router DIR-853 to a cable or DSL modem or to a private Ethernet line and use a high-speed Internet connection to successfully fulfill a wide range of professional tasks. The built-in 4-port switch enables you to connect Ethernet-enabled computers, game consoles, and other devices to your network.

Using the DIR-853 device, you are able to quickly create a high-speed wireless network at home or in your office, which lets computers and mobile devices access the Internet virtually anywhere (within the operational range of your wireless network). Simultaneous activity of 2.4GHz band and 5GHz band allows performing a wide range of tasks. The router can operate as a base station for connecting wireless devices of the standards 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac (at the wireless connection rate up to 1300Mbps[2]).

The router supports multiple functions for the wireless interface: several security standards (WEP, WPA/WPA2), MAC address filtering, WPS, WMM.

In addition, the device is equipped with a button for switching the Wi-Fi network off/on. If needed, for example, when you leave home, you can easily switch the router’s WLAN by pressing the button, and devices connected to the LAN ports of the router will stay online.

Multi-user MIMO technology allows to distribute the router's resources to let multiple wireless clients use the Wi-Fi network efficiently, keeping high rates for HD media streaming, lag-free gaming, and fast transfer of large files.

Transmit Beamforming technology allows to flexibly change the antennas' radiation pattern and to redistribute the signal directly to wireless devices connected to the router.

Smart adjustment of Wi-Fi clients is useful for networks based on several D-Link access points or routers – when the smart adjustment function is configured on each of them, a client always connects to the access point (router) with the highest signal level.

Support of guest Wi-Fi network allows you to create a separate wireless network with individual security settings. Devices connected to the guest network will be able to access the Internet, but will be isolated from the devices and resources of the router's LAN.

The wireless router DIR-853 includes a built-in firewall. The advanced security functions minimize threats of hacker attacks, prevent unwanted intrusions to your network, and block access to unwanted websites for users of your LAN.

In addition, the router supports IPsec and allows to create secure VPN tunnels.

[1] Not included in the delivery package. D-Link does not guarantee compatibility with all USB modems. For the list of supported USB modems, see the ***Specifications**** section, page 8.

[2] Up to 450Mbps for 2.4GHz and up to 867Mbps for 5GHz.

Built-in Yandex.DNS service protects against malicious and fraudulent web sites and helps to block access to adult content on children's devices.

The router also supports the SafeDNS/SkyDNS web content filtering services, which provide more settings and opportunities for safer Internet experience for home users of all ages and for professional activities of corporate users.

You can configure the settings of the wireless router DIR-853 via the user-friendly web-based interface (the interface is available in two languages – in Russian and in English).

The configuration wizard allows you to quickly switch DIR-853 to one of the following modes: router (for connection to a wired or wireless ISP), access point, repeater, or client, and then configure all needed setting for operation in the selected mode in several simple steps.

Also DIR-853 supports configuration and management via D-Link Click'n'Connect mobile application for Android smartphones.

You can simply update the firmware: the router itself finds approved firmware on D-Link update server and notifies when ready to install it.

Specifications[*]

Hardware	
Processor	· MT7621A (880MHz, dual core)
RAM	· 128MB, DDR3
Flash	· 16MB, SPI
Interfaces	· 10/100/1000BASE-T WAN port · 4 10/100/1000BASE-T LAN ports · USB 3.0 port
LEDs	· POWER · INTERNET · WPS · WLAN 2.4G · WLAN 5G · 4 LAN LEDs · USB
Buttons	· POWER button to power on/power off · WiFi button to enable/disable wireless network · WPS button to set up wireless connection · RESET button to restore factory default settings
Antenna	· Four external non-detachable antennas (5dBi gain)
MIMO	· 2 x 2, MU-MIMO
Power connector	· Power input connector (DC)

Software	
WAN connection types	· LTE · 3G · PPPoE · IPv6 PPPoE · PPPoE Dual Stack · Static IPv4 / Dynamic IPv4 · Static IPv6 / Dynamic IPv6 · PPPoE + Static IP (PPPoE Dual Access) · PPPoE + Dynamic IP (PPPoE Dual Access) · PPTP/L2TP + Static IP · PPTP/L2TP + Dynamic IP

[*] The device features are subject to change without notice. For the latest versions of the firmware and relevant documentation, visit www.dlink.ru.

Software	
Network functions	· Support of IEEE 802.1X for Internet connection · DHCP server/relay · Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation · Automatic obtainment of LAN IP address (for access point/repeater/client modes) · DNS relay · Dynamic DNS · Static IP routing · Static IPv6 routing · IGMP Proxy · RIP · Support of UPnP IGD · Support of VLAN · WAN ping respond · Support of SIP ALG · Support of RTSP · WAN reservation · Built-in UDPXY application · XUPNPD plug-in
Firewall functions	· Network Address Translation (NAT) · Stateful Packet Inspection (SPI) · IP filter · IPv6 filter · MAC filter · URL filter · DMZ · Prevention of ARP and DDoS attacks · Virtual servers · Built-in Yandex.DNS web content filtering service · Built-in SafeDNS web content filtering service
VPN	· IPsec/PPTP/L2TP/PPPoE pass-through · IPsec tunnels
USB interface functions	· USB modem Auto connection to available type of supported network (4G/3G/2G) Auto configuration of connection upon plugging in USB modem Enabling/disabling PIN code check, changing PIN code[3] · USB storage File browser Print server Access to storage via accounts Built-in Samba/FTP/DLNA server Built-in Transmission torrent client; uploading/downloading files from/to USB storage
Management	· Local and remote access to settings through TELNET/WEB (HTTP/HTTPS) · Bilingual web-based interface for configuration and management (Russian/English) · Support of Click'n'Connect application for Android smartphones · Notification on connection problems and auto redirect to settings · Firmware update via web-based interface · Automatic notification on new firmware version · Saving/restoring configuration to/from file · Support of logging to remote host/connected USB storage · Automatic synchronization of system time with NTP server and manual time/date setup · Ping utility · Traceroute utility · TR-069 client

[3] For GSM USB modems and some models of LTE USB modems.

Wireless Module Parameters	
Standards	· IEEE 802.11a/n/ac · IEEE 802.11b/g/n
Frequency range	· 2400 ~ 2483.5MHz · 5150 ~ 5350MHz · 5650 ~ 5725MHz
Wireless connection security	· WEP · WPA/WPA2 (Personal/Enterprise) · MAC filter · WPS (PBC/PIN)
Advanced functions	· Support of client mode · WMM (Wi-Fi QoS) · Information on connected Wi-Fi clients · Advanced settings · Smart adjustment of Wi-Fi clients · Guest Wi-Fi / support of MBSSID · Periodic scan of channels, automatic switch to least loaded channel · Support of 802.11ac (5GHz) and 802.11n (2.4GHz) TX Beamforming
Wireless connection rate[4]	· IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54Mbps · IEEE 802.11b: 1, 2, 5.5, and 11Mbps · IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps · IEEE 802.11n (2.4GHz): 6,5–300Mbps (MCS0–MCS15) to 450Mbps (QAM256) · IEEE 802.11n (5GHz): from 6,5 to 300Mbps (from MCS0 to MCS15) · IEEE 802.11ac (5GHz): from 6,5 to 867Mbps (from MCS0 to MSC9)
Transmitter output power *The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country*	· 802.11a (typical at room temperature 25 °C) 15dBm at 6, 9, 12, 18, 24, 36, 48, 54Mbps · 802.11b (typical at room temperature 25 °C) 15dBm at 1, 2, 5.5, 11Mbps · 802.11g (typical at room temperature 25 °C) 15dBm at 6, 9, 12, 18, 24, 36, 48, 54Mbps · 802.11n (typical at room temperature 25 °C) 2.4GHz 15dBm at MCS0~7 5GHz 15dBm at MCS0~7 · 802.11ac (typical at room temperature 25 °C) 15dBm at MCS0~9

[4] Maximum wireless signal rate is derived from IEEE standard 802.11ac and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

Wireless Module Parameters	
Receiver sensitivity	· 802.11a -96dBm at 6Mbps -94dBm at 9Mbps -92dBm at 12Mbps -90dBm at 18Mbps -88dBm at 24Mbps -84dBm at 36Mbps -80dBm at 48Mbps -78dBm at 54Mbps · 802.11b -94dBm at 1Mbps -92dBm at 2Mbps -90dBm at 5.5Mbps -87dBm at 11Mbps · 802.11g -92dBm at 6Mbps -90dBm at 9Mbps -88dBm at 12Mbps -86dBm at 18Mbps -84dBm at 24Mbps -80dBm at 36Mbps -77dBm at 48Mbps -74dBm at 54Mbps · 802.11n 2.4GHz -89dBm at MCS0 -86dBm at MCS1 -84dBm at MCS2 -81dBm at MCS3 -78dBm at MCS4 -74dBm at MCS5 -72dBm at MCS6 -70dBm at MCS7 5GHz -92dBm at MCS0 -89dBm at MCS1 -86dBm at MCS2 -84dBm at MCS3 -80dBm at MCS4 -76dBm at MCS5 -75dBm at MCS6 -73dBm at MCS7 · 802.11ac -90dBm at MCS0 -87dBm at MCS1 -84dBm at MCS2 -81dBm at MCS3 -78dBm at MCS4 -73dBm at MCS5 -72dBm at MCS6 -70dBm at MCS7 -67dBm at MCS8 -65dBm at MCS9
Modulation schemes	· 802.11a: BPSK, QPSK, 16QAM, 64QAM with OFDM · 802.11b: DQPSK, DBPSK, DSSS, CCK · 802.11g: BPSK, QPSK, 16QAM, 64QAM with OFDM · 802.11n: BPSK, QPSK, 16QAM, 64QAM, 256QAM with OFDM · 802.11ac: BPSK, QPSK, 16QAM, 64QAM, up to 256QAM with OFDM

Physical Parameters	
Dimensions (L x W x H)	· 213 x 140 x 33 mm (8.39 x 5.51 x 1.3 in)
Weight	· 350 g (0.77 lb)

Operating Environment	
Power	· Output: 12V DC, 1.5A
Temperature	· Operating: from 0 to 40 °C · Storage: from -20 to 65 °C
Humidity	· Operating: from 10% to 90% (non-condensing) · Storage: from 5% to 95% (non-condensing)

Supported USB modems[5]	
GSM	· Alcatel X500 · D-Link DWM-152C1 · D-Link DWM-156A6 · D-Link DWM-156A7 · D-Link DWM 156A8 · D-Link DWM-156C1 · D-Link DWM-157B1 · D-Link DWM-157B1 (Velcom) · D-Link DWM-158D1 · D-Link DWR-710 · Huawei E150 · Huawei E1550 · Huawei E156G · Huawei E160G · Huawei E169G · Huawei E171 · Huawei E173 (Megafon) · Huawei E220 · Huawei E3131 (MTS 420S) · Huawei E352 (Megafon) · Prolink PHS600 · Prolink PHS901 · ZTE MF112 · ZTE MF192 · ZTE MF626 · ZTE MF627 · ZTE MF652 · ZTE MF667 · ZTE MF668 · ZTE MF752

[5] The manufacturer does not guarantee proper operation of the router with every modification of the firmware of USB modems.

Supported USB modems	
LTE	· Huawei E3131 · Huawei E3272 · Huawei E3351 · Huawei E3372 · Huawei E367 · Huawei E392 · Megafon M100-1 · Megafon M100-2 · Megafon M100-3 · Megafon M100-4 · Megafon M150-1 · Megafon M150-2 · Quanta 1K6E (Beeline 1K6E) · MTS 824F · MTS 827F · Yota LU-150 · Yota WLTUBA-107 · ZTE MF823 · ZTE MF827
Smartphones in USB tethering mode	· Some models of Android smartphones

Product Appearance

Upper and Front Panels

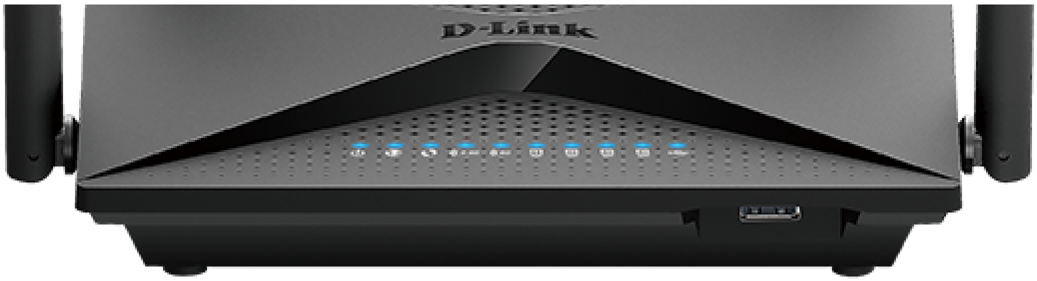


Figure 1. Upper and front panels view.

LED	Mode	Description
POWER	*Solid orange*	The router is being loaded.
	Solid blue	The router is powered on.
	No light	The router is powered off.
INTERNET	*Solid blue*	• The default wired WAN connection is on, or • the default 3G/LTE WAN connection is on.
	Fast blinking blue	• The default wired WAN connection is active, or • the default 3G/LTE WAN connection is active.
	Blinking orange	• The default wired WAN connection is off, or • there are no WAN connections created.
	No light	The WAN cable is not connected.
WPS	*Blinking blue*	Attempting to add a wireless device via the WPS function.
	No light	The WPS function is not in use.
2.4G WLAN **5G WLAN**	*Solid blue*	The router's WLAN of the relevant band is on.
	Blinking blue	The WLAN interface of the relevant band is active (upstream or downstream traffic).
	No light	The router's WLAN of the relevant band is off.

LED	Mode	Description
LAN 1-4	*Solid blue*	A device (computer) is connected to the relevant port, the connection is on.
	Blinking blue	The LAN port is active (upstream or downstream traffic).
	No light	The cable is not connected to the relevant port.
USB	*Solid blue*	A USB device is connected to the router's USB port.
	No light	No USB device.

The **USB** port located on the front panel of the router is designed to connect a USB device (modem, storage, printer).

Back Panel

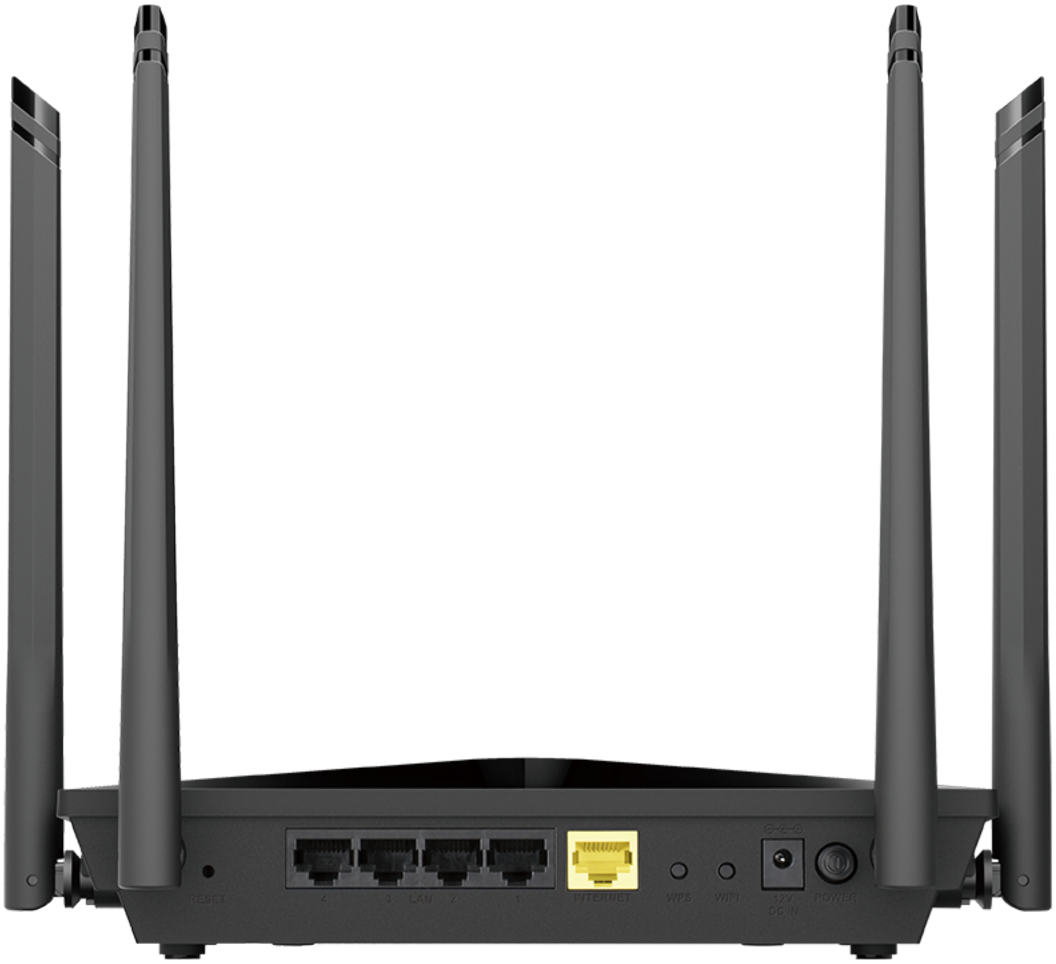


Figure 2. Back panel view.

Port	Description
RESET	A button to restore the factory defaults. To restore the factory defaults, push the button (with the device turned on), hold it for 10 seconds, and then release the button.
LAN 1-4	4 Ethernet ports to connect computers or network devices.
INTERNET	A port to connect to a cable or DSL modem or to a private Ethernet line (it is recommended to use the cable included in the delivery package).

Port	Description
WPS	A button to set up wireless connection (the WPS function). To use the WPS function: with the device turned on, push the button, hold it for 2 seconds, and release. The **WPS** LED should start blinking.
WIFI	A button to enable/disable wireless network. To disable the router's wireless network: with the device turned on, press the button and release. The **2.4G WLAN** and **5G WLAN** LEDs should turn off.
12V DC IN	Power connector.
POWER	A button to turn the router on/off.

The device is also equipped with four external non-detachable Wi-Fi antennas.

Delivery Package

The following should be included:

- Router DIR-853
- Power adapter DC 12V/1.5A
- Ethernet cable (CAT 5E)
- "***Quick Installation Guide***" (brochure).

The "***User Manual***" and "***Quick Installation Guide***" documents are available on D-Link website (see www.dlink.ru).

! Using a power supply with a different voltage rating than the one included will cause damage and void the warranty for this product.

CHAPTER 3. INSTALLATION AND CONNECTION

Before You Begin

Please, read this manual prior to installing the device. Make sure that you have all the necessary information and equipment.

Operating System

Configuration of the wireless dual band gigabit router with 3G/LTE support DIR-853 (hereinafter referred to as “the router”) is performed via the built-in web-based interface. The web-based interface is available from any operating system that supports a web browser.

Web Browser

The following web browsers are recommended:

- Apple Safari 8 and later
- Google Chrome 48 and later
- Microsoft Internet Explorer 10 and later
- Microsoft Edge 20.10240 and later
- Mozilla Firefox 44 and later
- Opera 35 and later.

For successful operation, JavaScript should be enabled on the web browser. Make sure that JavaScript has not been disabled by other software (such as virus protection or web user security packages) running on your computer.

Wired or Wireless NIC (Ethernet or Wi-Fi Adapter)

Any computer that uses the router should be equipped with an Ethernet or Wi-Fi adapter (NIC). If your computer is not equipped with such a device, install an Ethernet or Wi-Fi adapter prior to using the router.

Wireless Connection

Wireless workstations from your network should be equipped with a wireless 802.11a, b, g, n, or ac NIC (Wi-Fi adapter). In addition, you should specify the values of SSID, channel number and security settings defined in the web-based interface of the router for all these wireless workstations.

USB Modem

To connect to an LTE or 3G network, you should use a USB modem. Connect it to the USB port of the router, then access the web-based interface of the router, and you will be able to configure a connection to the Internet[6].

Your USB modem should be equipped with an active SIM card of your operator.

Some operators require subscribers to activate their USB modems prior to using them. Please, refer to connection guidelines provided by your operator when concluding the agreement or placed on its website.

For some models of LTE USB modems, it is required to disable the PIN code check on the SIM card prior to connecting the USB modem to the router.

[6] Contact your operator to get information on the service coverage and fees.

Connecting to PC

PC with Ethernet Adapter

1. Make sure that your PC is powered off.
2. Connect an Ethernet cable between any of LAN ports located on the back panel of the router and the Ethernet port of your PC.
3. ***To connect via USB modem***: connect your USB modem to the USB port[7] located on the front panel of the router.

! In some cases you will need to reboot the router after connection of the USB modem.

4. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.
5. Turn on the router by pressing the **POWER** button on its back panel.
6. Turn on your PC and wait until your operating system is completely loaded.

[7] It is recommended to use a USB extension cable to connect a USB modem to the router.

Obtaining IP Address Automatically in OS Windows XP

1. Click the **Start** button and proceed to the **Control Panel > Network and Internet Connections > Network Connections** window.
2. In the **Network Connections** window, right-click the relevant **Local Area Connection** icon and select the **Properties** line in the menu displayed.

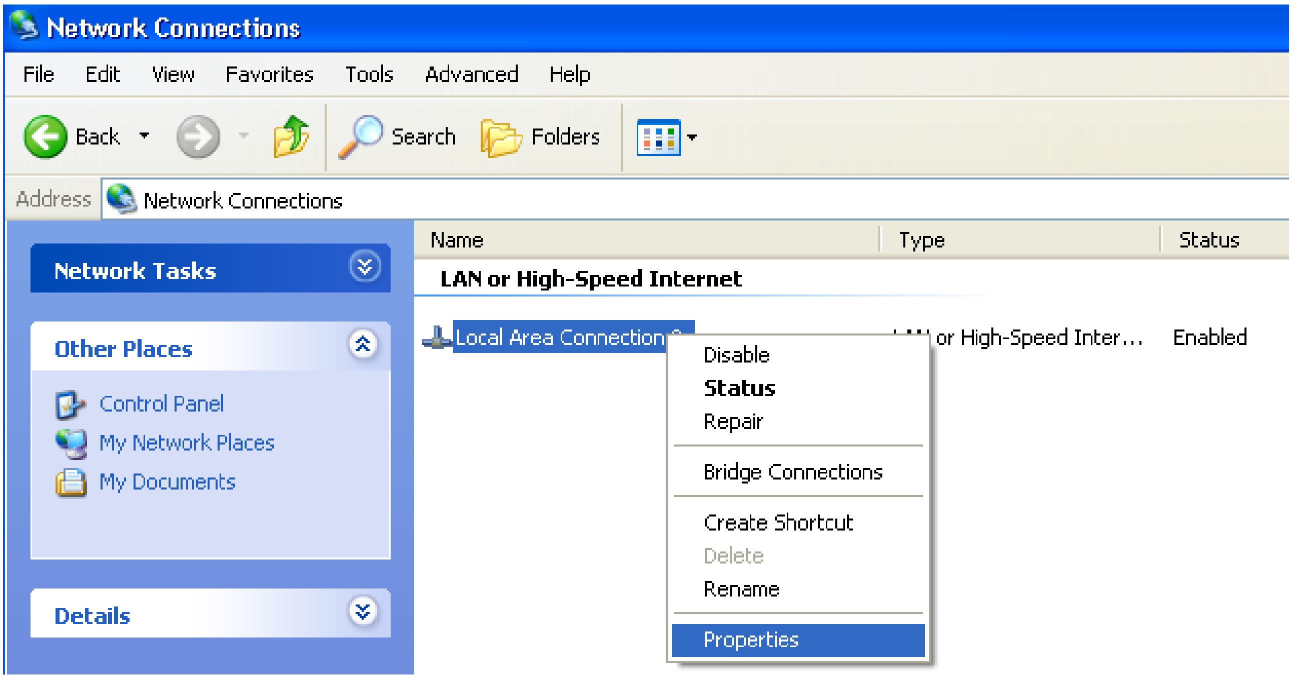
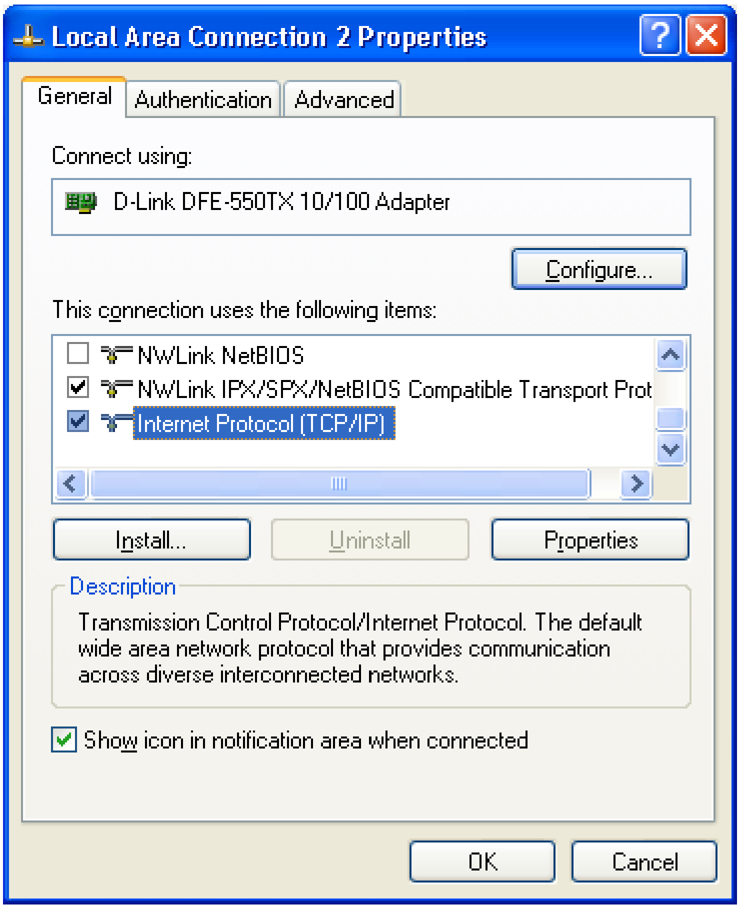


*Figure 3. The **Network Connections** window.*

3. In the **Local Area Connection Properties** window, on the **General** tab, select the **Internet Protocol (TCP/IP)** line. Click the **Properties** button.



Connect using:

D-Link DFE-550TX 10/100 Adapter

This connection uses the following items:

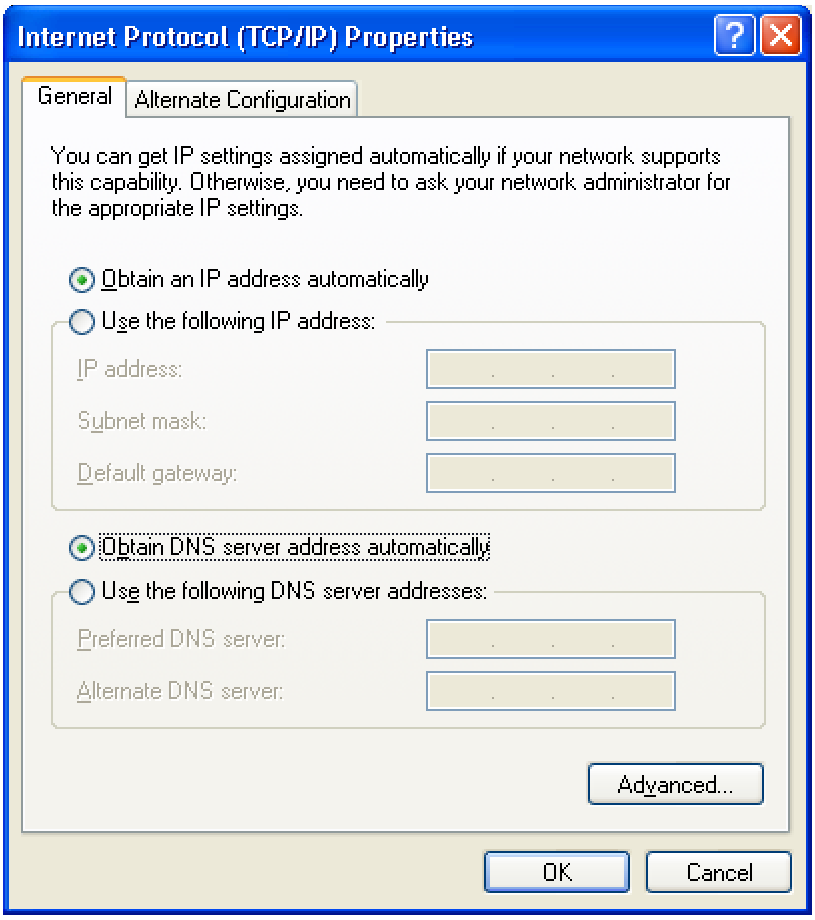
☐ NWLink NetBIOS
☑ NWLink IPX/SPX/NetBIOS Compatible Transport Prot
☑ Internet Protocol (TCP/IP)

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

*Figure 4. The **Local Area Connection Properties** window.*

4. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. Click the **OK** button.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

*Figure 5. The **Internet Protocol (TCP/IP) Properties** window.*

5. Click the **OK** button in the connection properties window.

Now your computer is configured to obtain an IP address automatically.

Obtaining IP Address Automatically in OS Windows 7

1. Click the **Start** button and proceed to the **Control Panel** window.
2. Select the **Network and Sharing Center** section. (If the Control Panel has the category view (the **Category** value is selected from the **View by** drop-down list in the top right corner of the window), choose the **View network status and tasks** line under the **Network and Internet** section.)

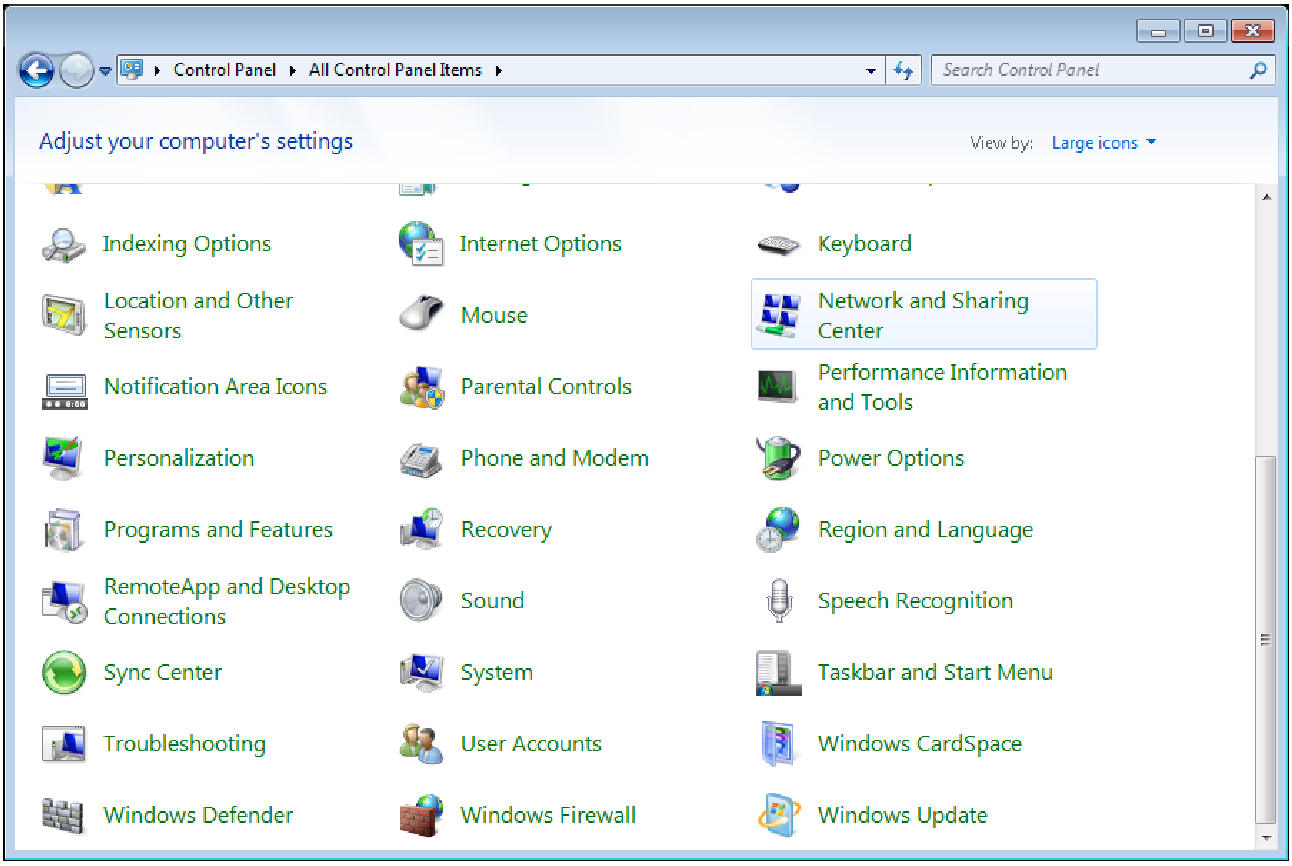
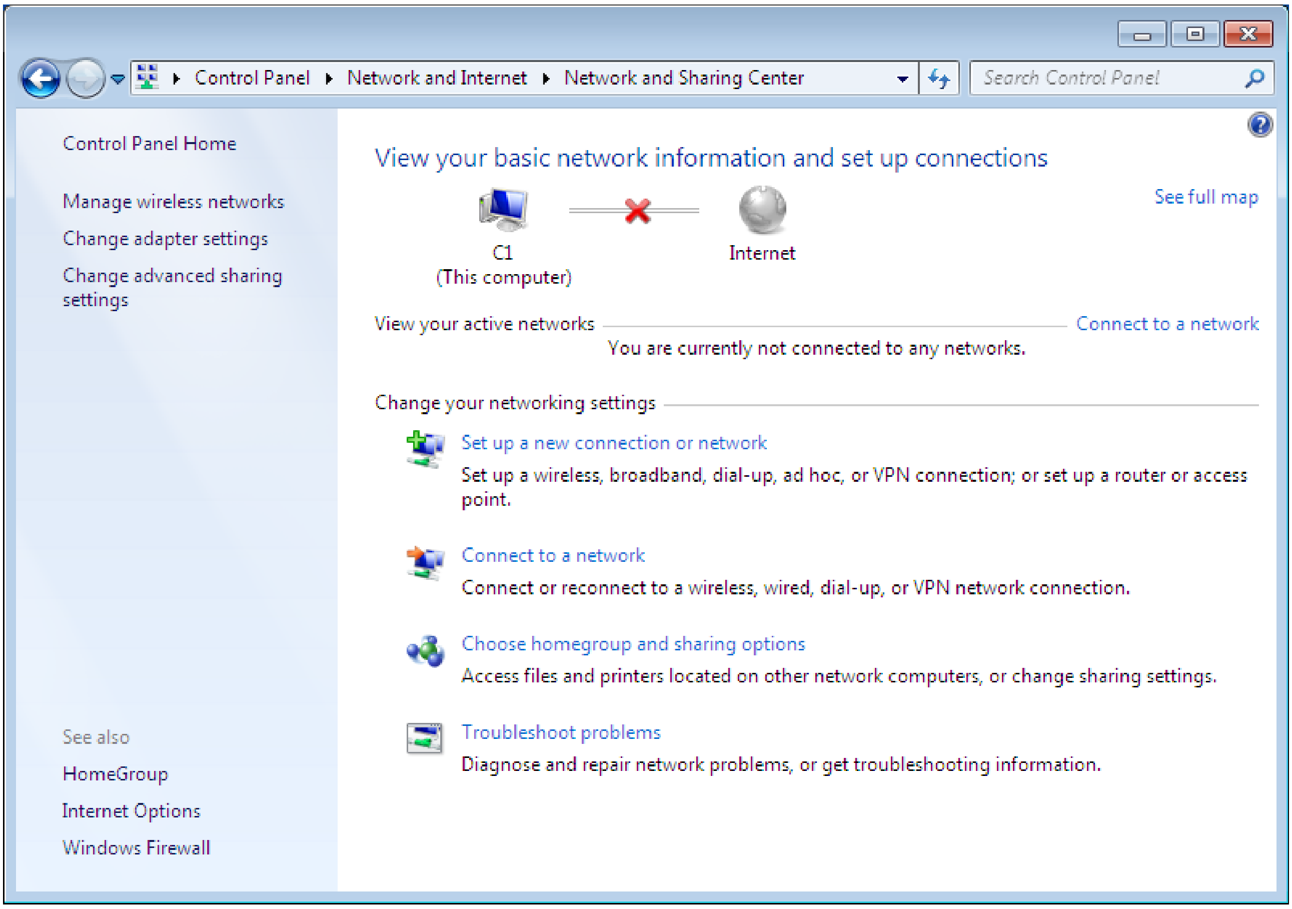


*Figure 6. The **Control Panel** window.*

3. In the menu located on the left part of the window, select the **Change adapter settings** line.



View your basic network information and set up connections

View your active networks

You are currently not connected to any networks.

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

*Figure 7. The **Network and Sharing Center** window.*

4. In the opened window, right-click the relevant **Local Area Connection** icon and select the **Properties** line in the menu displayed.

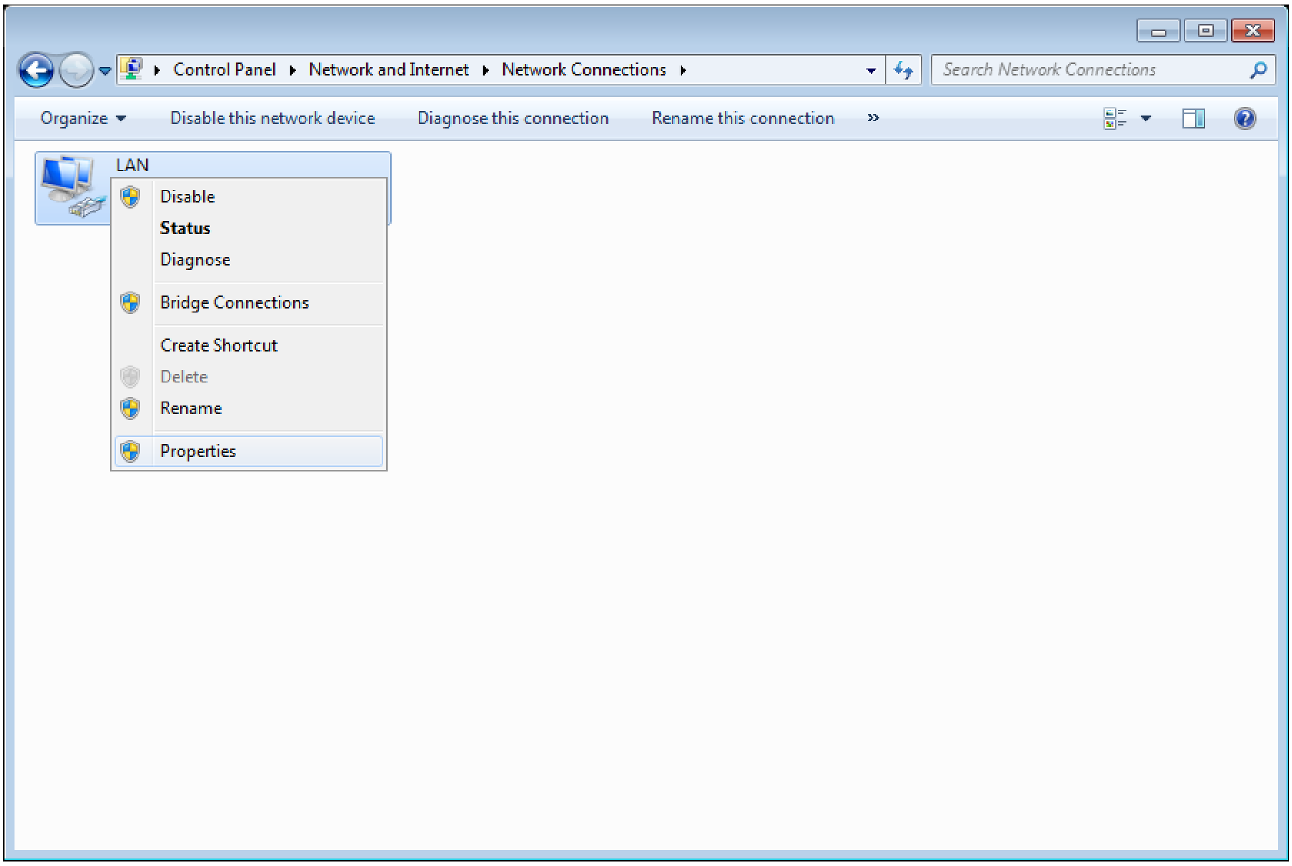
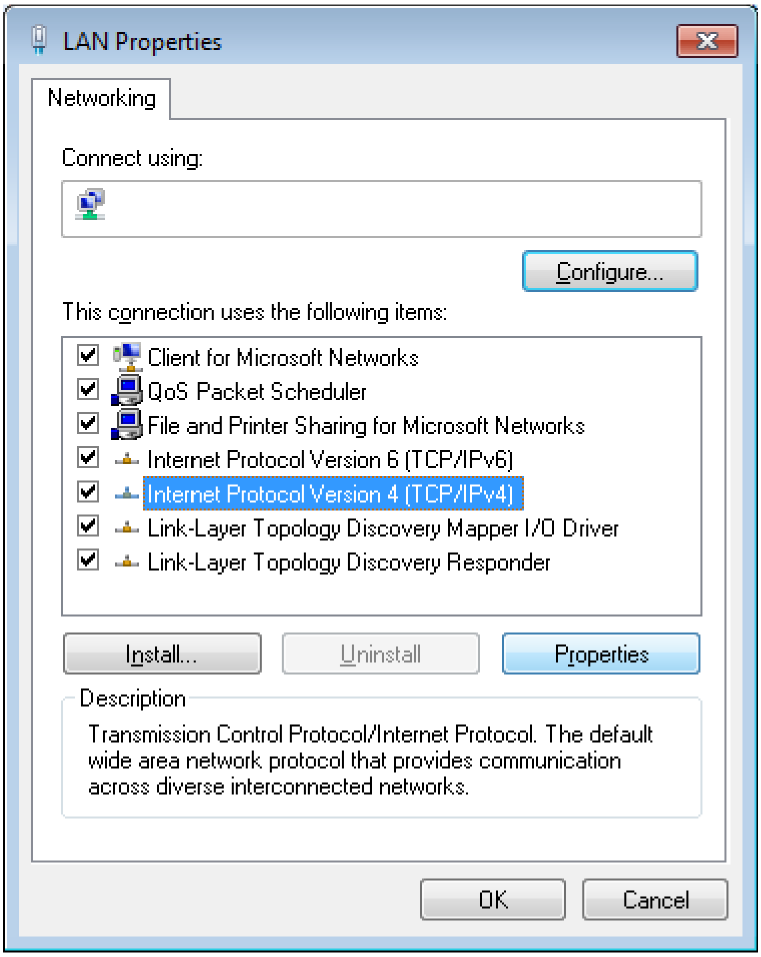


*Figure 8. The **Network Connections** window.*

5. In the **Local Area Connection Properties** window, on the **Networking** tab, select the **Internet Protocol Version 4 (TCP/IPv4)** line. Click the **Properties** button.



LAN Properties

Networking

Connect using:

This connection uses the following items:

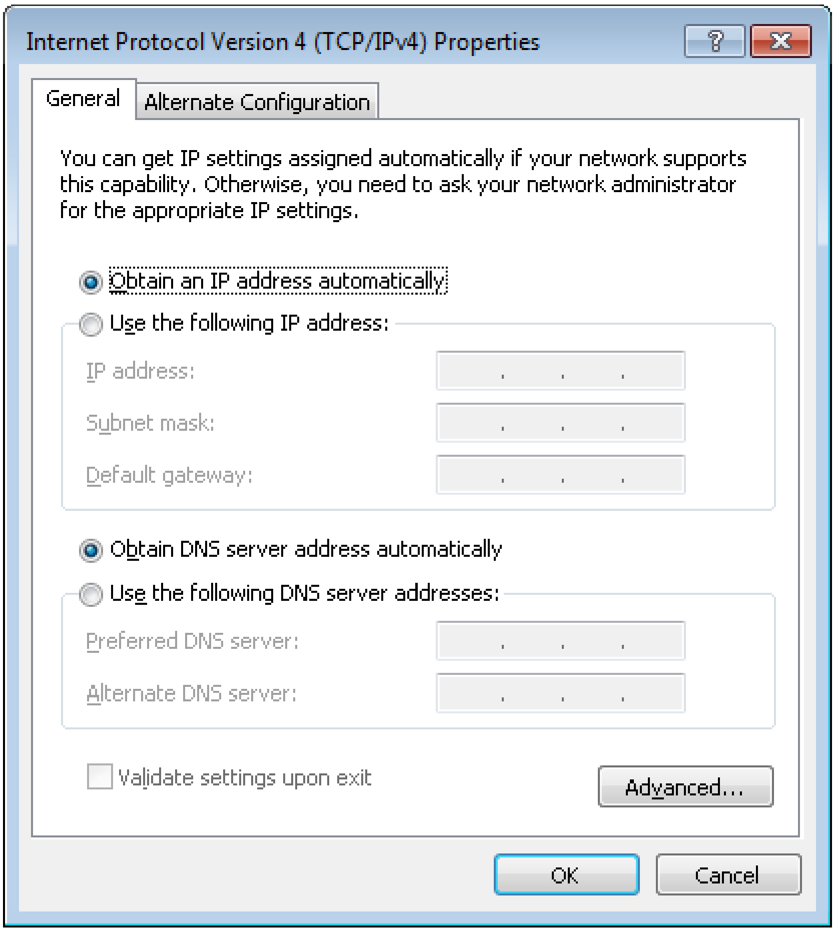
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

*Figure 9. The **Local Area Connection Properties** window.*

6. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. Click the **OK** button.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Figure 10. The ***Internet Protocol Version 4 (TCP/IPv4) Properties*** *window.*

7. Click the **OK** button in the connection properties window.

Now your computer is configured to obtain an IP address automatically.

PC with Wi-Fi Adapter

1. ***To connect via USB modem***: connect your USB modem to the USB port[8] located on the front panel of the router.

! In some cases you will need to reboot the router after connection of the USB modem.

2. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.
3. Turn on the router by pressing the **POWER** button on its back panel.
4. Turn on your PC and wait until your operating system is completely loaded.
5. Turn on your Wi-Fi adapter. As a rule, modern notebooks with built-in wireless NICs are equipped with a button or switch that turns on/off the wireless adapter (refer to your PC documents). If your PC is equipped with a pluggable wireless NIC, install the software provided with your Wi-Fi adapter.

[8] It is recommended to use a USB extension cable to connect a USB modem to the router.

Configuring Wi-Fi Adapter in OS Windows XP

1. Click the **Start** button and proceed to the **Control Panel > Network and Internet Connections > Network Connections** window.
2. Select the icon of the wireless network connection and make sure that your Wi-Fi adapter is on.

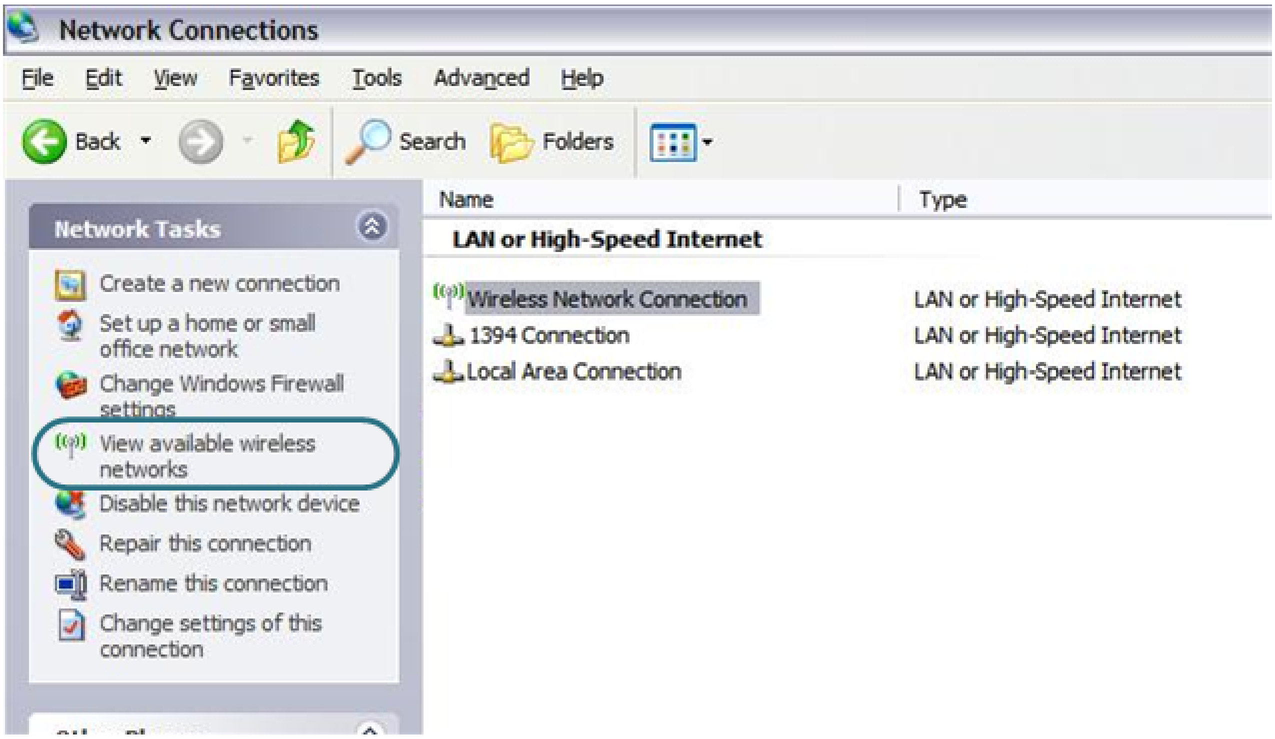

Network Connections
File
Edit
View
Favorites
Tools
Advanced
Help
Back
Search
Folders
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
View available wireless networks
Disable this network device
Repair this connection
Rename this connection
Change settings of this connection
Name
Type
LAN or High-Speed Internet
Wireless Network Connection
1394 Connection
Local Area Connection
LAN or High-Speed Internet
LAN or High-Speed Internet
LAN or High-Speed Internet

Figure 11. The ***Network Connections*** *window.*

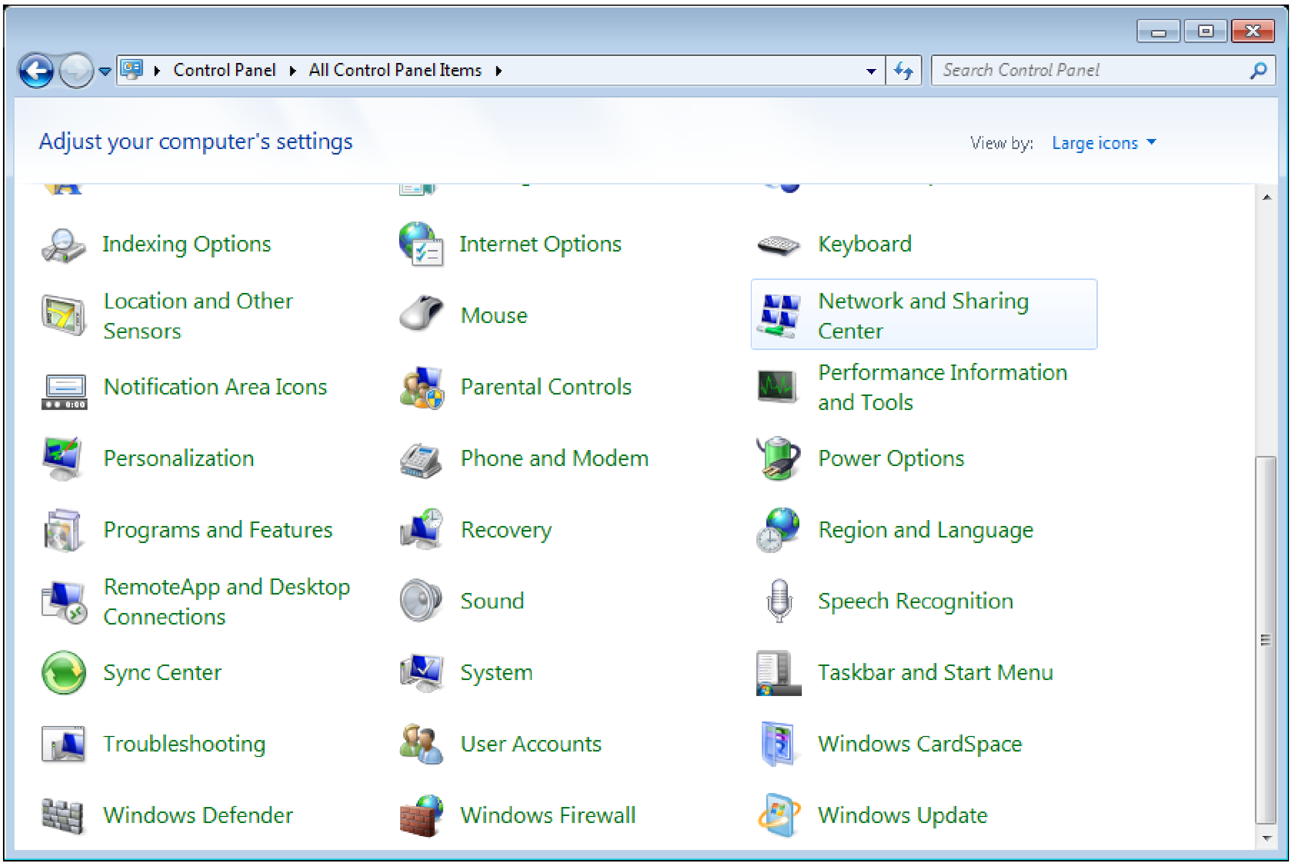
3. Search for available wireless networks.
4. In the opened **Wireless Network Connection** window, select the wireless network `DIR-853` (for operating in the 2.4GHz band) or `DIR-853-5G` (for operating in the 5GHz band) and click the **Connect** button.
5. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) in the **Network key** and **Confirm network key** fields and click the **Connect** button.

After that the **Wireless Network Connection Status** window appears.

! If you perform initial configuration of the router via Wi-Fi connection, note that immediately after changing the wireless default settings of the router you will need to reconfigure the wireless connection using the newly specified settings.

Configuring Wi-Fi Adapter in OS Windows 7

1. Click the **Start** button and proceed to the **Control Panel** window.
2. Select the **Network and Sharing Center** section. (If the Control Panel has the category view (the **Category** value is selected from the **View by** drop-down list in the top right corner of the window), choose the **View network status and tasks** line under the **Network and Internet** section.)



Control Panel ▸ All Control Panel Items ▸

Search Control Panel

Adjust your computer's settings

View by: Large icons

Indexing Options	Internet Options	Keyboard
Location and Other Sensors	Mouse	Network and Sharing Center
Notification Area Icons	Parental Controls	Performance Information and Tools
Personalization	Phone and Modem	Power Options
Programs and Features	Recovery	Region and Language
RemoteApp and Desktop Connections	Sound	Speech Recognition
Sync Center	System	Taskbar and Start Menu
Troubleshooting	User Accounts	Windows CardSpace
Windows Defender	Windows Firewall	Windows Update

*Figure 12. The **Control Panel** window.*

3. In the menu located on the left part of the window, select the **Change adapter settings** line.
4. In the opened window, select the icon of the wireless network connection and make sure that your Wi-Fi adapter is on.
5. To open the list of available wireless networks, select the icon of the wireless network connection and click the **Connect To** button or left-click the network icon in the notification area located on the right side of the taskbar.

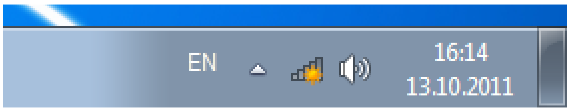


Figure 13. The notification area of the taskbar.

6. In the opened **Wireless Network Connection** window, select the wireless network **`DIR-853`** (for operating in the 2.4GHz band) or **`DIR-853-5G`** (for operating in the 5GHz band) and click the **Connect** button.

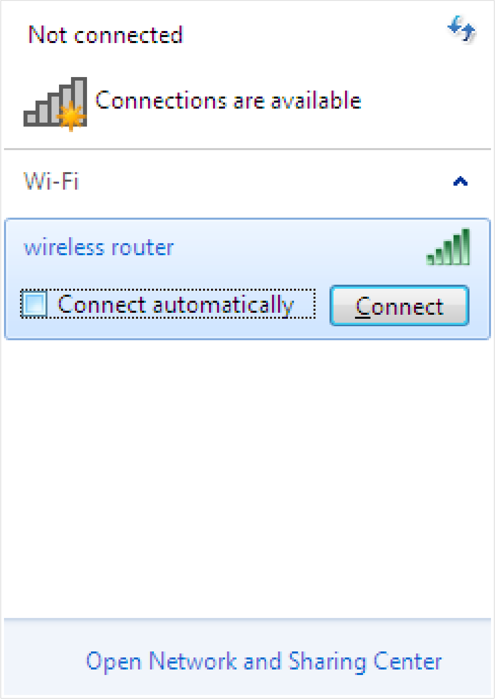


Figure 14. The list of available networks.

7. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) in the **Security key** field and click the **OK** button.
8. Wait for about 20-30 seconds. After the connection is established, the network icon will be displayed as the signal level scale.

! <u>If you perform initial configuration of the router via Wi-Fi connection, note that immediately after changing the wireless default settings of the router you will need to reconfigure the wireless connection using the newly specified settings.</u>

Connecting to Web-based Interface

When you have configured your computer, you can access the web-based interface and configure needed parameters (create a WAN connection, change the parameters of the wireless network, specify the settings of the firewall, etc.).

! For security reasons, DIR-853 with default settings cannot connect to the Internet. To get started, please set your own password used to access the web-based interface and, if needed, configure other settings recommended by your ISP.

Start a web browser (see the ***Before You Begin*** section, page 19). In the address bar of the web browser, enter the IP address of the router (by default, `192.168.0.1`) or its domain name (by default, `dlinkrouter.local`) with a dot at the end. Press the **Enter** key.

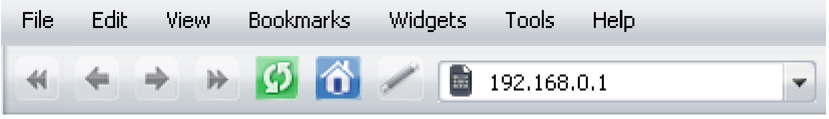
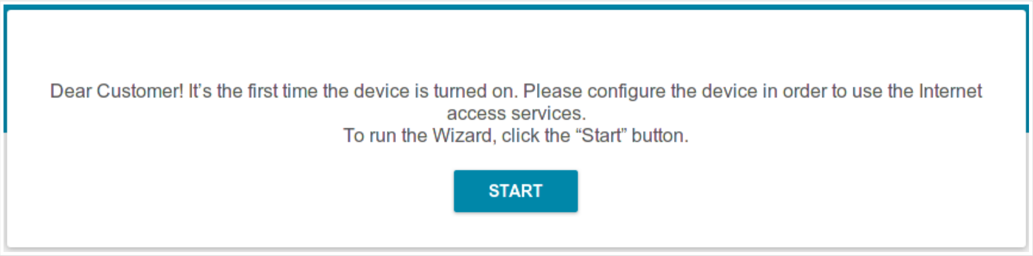


Figure 15. Connecting to the web-based interface of the DIR-853 device.

! If the error "*The page cannot be displayed*" (or "*Unable to display the page*"/"*Could not connect to remote server*") occurs upon connecting to the web-based interface of the router, make sure that you have properly connected the router to your computer.

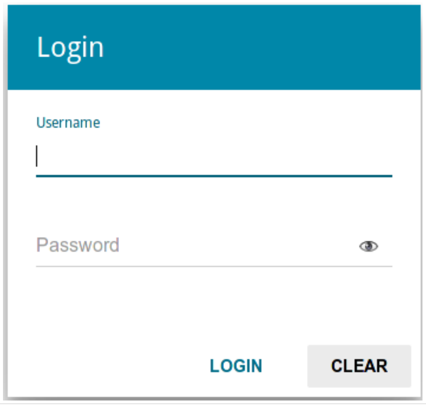
If the device has not been configured previously or the default settings have been restored, after access to the web-based interface the Initial Configuration Wizard opens (see the ***Initial Configuration Wizard*** section, page 41).



Dear Customer! It's the first time the device is turned on. Please configure the device in order to use the Internet access services.
To run the Wizard, click the "Start" button.

Figure 16. The page for running the Initial Configuration Wizard.

If you configured the device previously, after access to the web-based interface the login page opens. Enter the username (`admin`) in the **Username** field and the password you specified in the **Password** field, then click the **LOGIN** button.



Login

Username

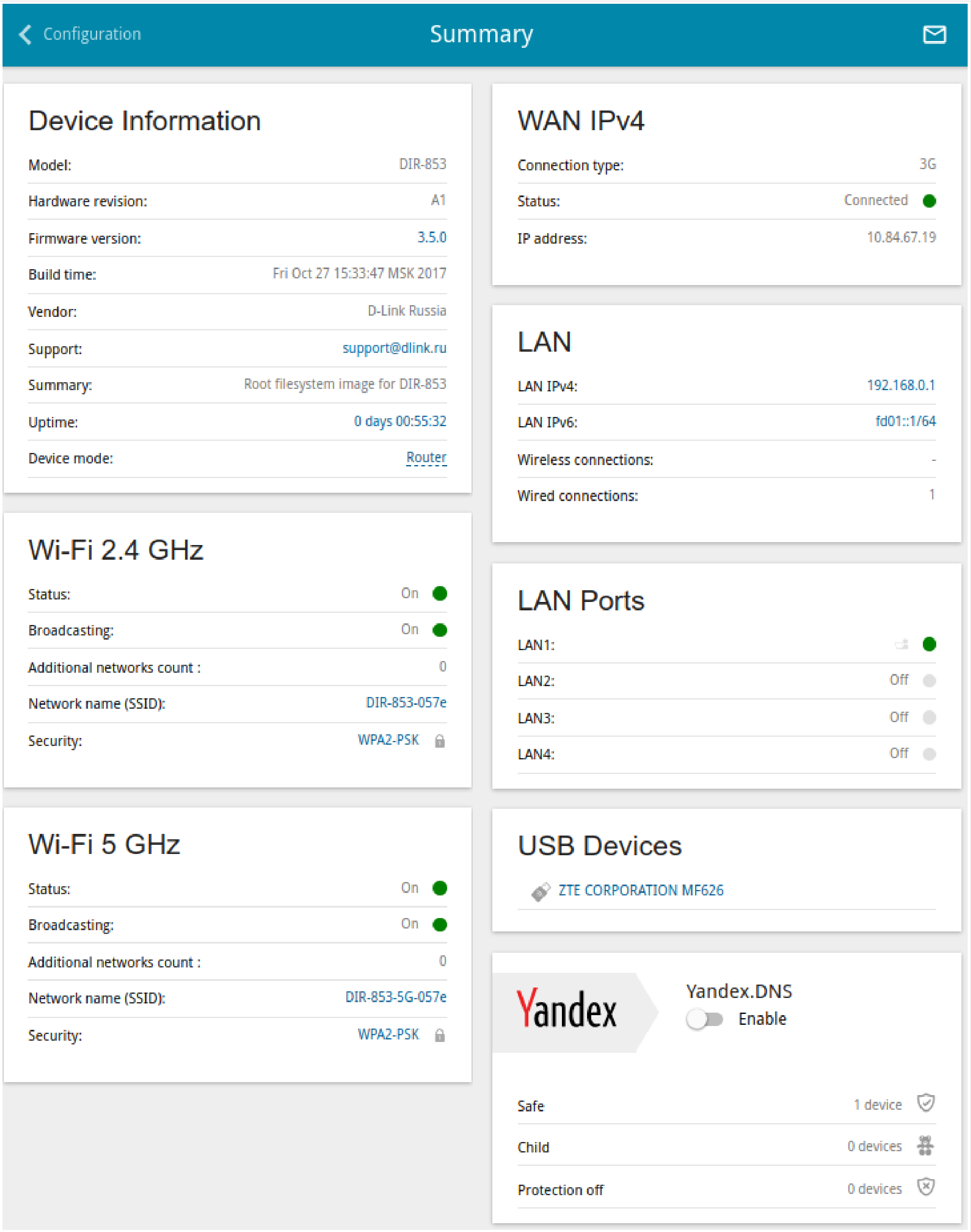
Password

Figure 17. The login page.

Web-based Interface Structure

Summary Page

On the **Summary** page, detailed information on the device state is displayed.



Configuration Summary

Device Information

Model:	DIR-853
Hardware revision:	A1
Firmware version:	3.5.0
Build time:	Fri Oct 27 15:33:47 MSK 2017
Vendor:	D-Link Russia
Support:	support@dlink.ru
Summary:	Root filesystem image for DIR-853
Uptime:	0 days 00:55:32
Device mode:	Router

WAN IPv4

Connection type:	3G
Status:	Connected ●
IP address:	10.84.67.19

LAN

LAN IPv4:	192.168.0.1
LAN IPv6:	fd01::1/64
Wireless connections:	-
Wired connections:	1

Wi-Fi 2.4 GHz

Status:	On ●
Broadcasting:	On ●
Additional networks count :	0
Network name (SSID):	DIR-853-057e
Security:	WPA2-PSK

LAN Ports

LAN1:	●
LAN2:	Off ○
LAN3:	Off ○
LAN4:	Off ○

Wi-Fi 5 GHz

Status:	On ●
Broadcasting:	On ●
Additional networks count :	0
Network name (SSID):	DIR-853-5G-057e
Security:	WPA2-PSK

USB Devices

ZTE CORPORATION MF626

Yandex Yandex.DNS

Enable

Safe	1 device
Child	0 devices
Protection off	0 devices

Figure 18. The summary page.

The **Device Information** section displays the model and hardware version of the router, the firmware version, and other data.

To contact the technical support group (to send an e-mail), left-click the support e-mail address. After clicking the line, the e-mail client window for sending a new letter to the specified address opens.

To change the operation mode of the device, left-click the name of the mode in the **Device mode** line. In the opened window, click the **initial setup wizard** link (for the detailed description of the Wizard, see the ***Initial Configuration Wizard*** section, page 41).

The **Wi-Fi 2.4 GHz** and **Wi-Fi 5 GHz** sections display data on the state of the device's wireless network, its name and the authentication type, and availability of an additional wireless network in the relevant band.

In the **WAN** section, data on the type and status of the existing WAN connection are displayed.

In the **LAN** section, the IPv4 and IPv6 address of the router and the number of wired and wireless clients of the device are displayed.

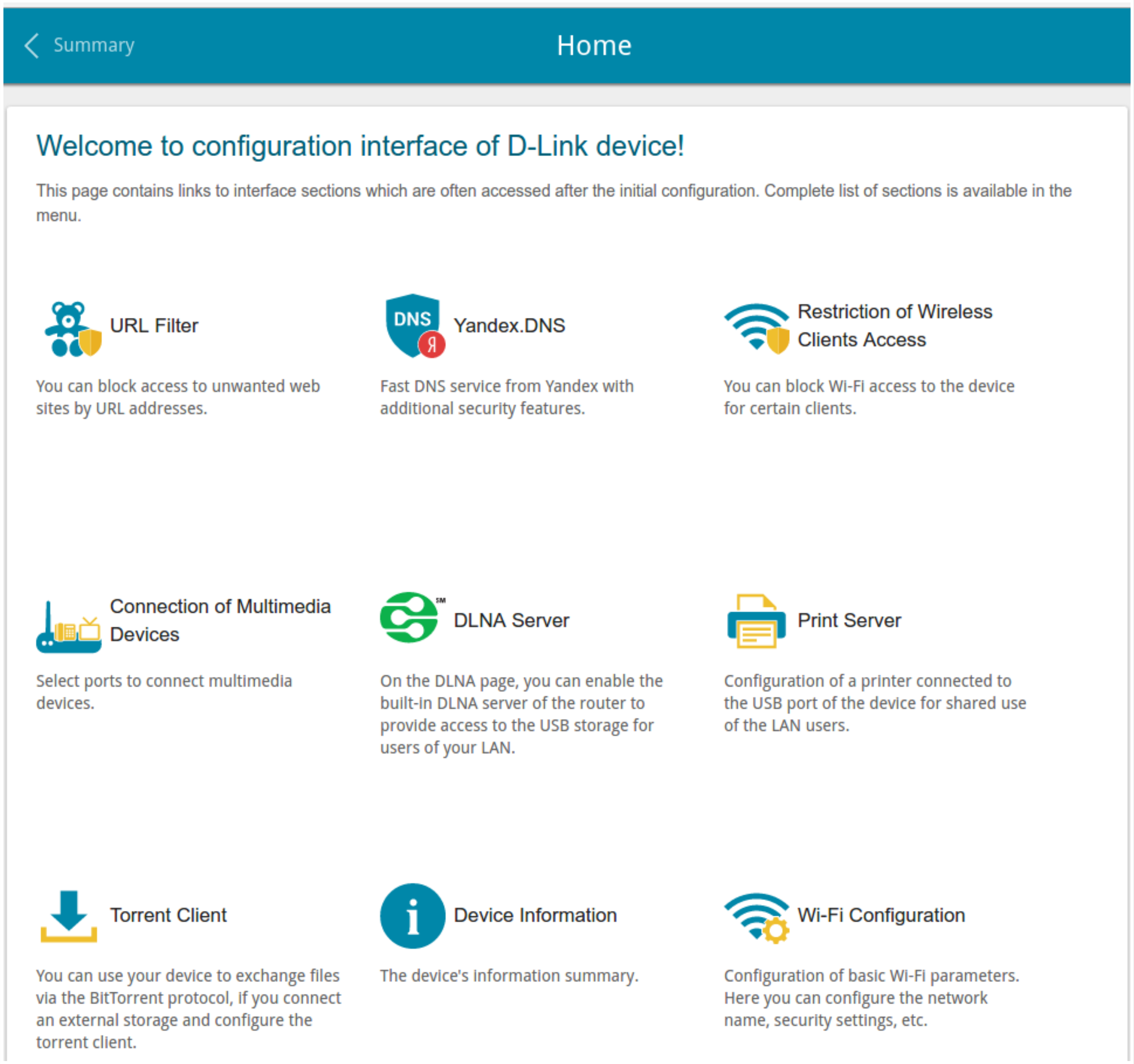
The **LAN Ports** section displays the state of the device's LAN ports and data transfer mode of active ports.

The **USB Devices** section displays the device connected to the USB port of the router.

The **Yandex.DNS** section displays the Yandex.DNS service state and operation mode. To enable the Yandex.DNS service, move the **Enable** switch to the right. If needed, change the operation mode of the service.

Home Page

The **Home** page displays links to the most frequently used pages with device's settings.



Welcome to configuration interface of D-Link device!

This page contains links to interface sections which are often accessed after the initial configuration. Complete list of sections is available in the menu.

URL Filter

You can block access to unwanted web sites by URL addresses.

Yandex.DNS

Fast DNS service from Yandex with additional security features.

Restriction of Wireless Clients Access

You can block Wi-Fi access to the device for certain clients.

Connection of Multimedia Devices

Select ports to connect multimedia devices.

DLNA Server

On the DLNA page, you can enable the built-in DLNA server of the router to provide access to the USB storage for users of your LAN.

Print Server

Configuration of a printer connected to the USB port of the device for shared use of the LAN users.

Torrent Client

You can use your device to exchange files via the BitTorrent protocol, if you connect an external storage and configure the torrent client.

Device Information

The device's information summary.

Wi-Fi Configuration

Configuration of basic Wi-Fi parameters. Here you can configure the network name, security settings, etc.

*Figure 19. The **Home** page.*

Other settings of the router are available in the menu in the left part of the page.

Menu Sections

To configure the router use the menu in the left part of the page.

In the **Initial Configuration** section you can run the Initial Configuration Wizard. The Wizard allows you to configure the router for operation in the needed mode and specify all parameters necessary for getting started (for the description of the Wizard, see the ***Initial Configuration Wizard*** section, page 41).

The pages of the **Statistics** section display data on the current state of the router (for the description of the pages, see the ***Statistics*** section, page 66).

The pages of the **Connections Setup** section are designed for configuring basic parameters of the LAN interface of the router and creating a connection to the Internet (for the description of the pages, see the ***Connections Setup*** section, page 72).

The pages of the **Wi-Fi** section are designed for specifying all needed settings of the router's wireless network (for the description of the pages, see the ***Wi-Fi*** section, page 112).

The **Print Server** section is designed for configuring the router as a print server (see the ***Print Server*** section, page 139).

The pages of the **USB Storage** section are designed for operating the connected USB storage (for the description of the pages, see the ***USB Storage*** section, page 140).

The pages of the **USB Modem** section are designed for operating the connected 3G or LTE USB modem (for the description of the pages, see the ***USB Modem*** section, page 152).

The pages of the **Advanced** section are designed for configuring additional parameters of the router (for the description of the pages, see the ***Advanced*** section, page 156).

The pages of the **Firewall** section are designed for configuring the firewall of the router (for the description of the pages, see the ***Firewall*** section, page 184).

The pages of the **System** section provide functions for managing the internal system of the router (for the description of the pages, see the ***System*** section, page 195).

The pages of the **Yandex.DNS** section are designed for configuring the Yandex.DNS web content filtering service (for the description of the pages, see the ***Yandex.DNS*** section, page 211).

To exit the web-based interface, click the **Logout** line of the menu.

Notifications

The router's web-based interface displays notifications in the top right part of the page.

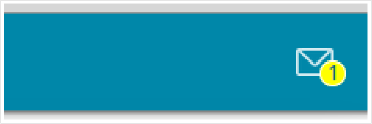


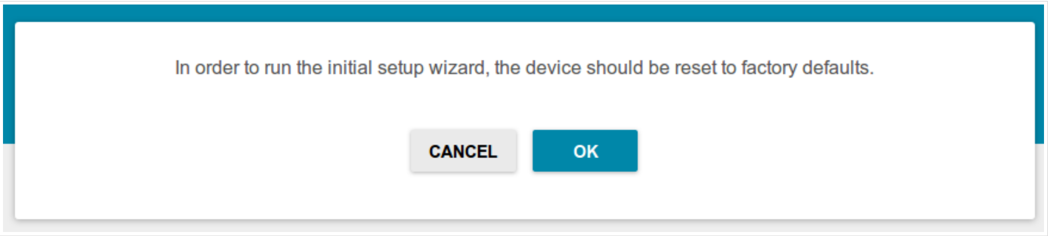
Figure 20. The web-based interface notifications.

Click the icon displaying the number of notifications to view the complete list and click the relevant button.

CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

Initial Configuration Wizard

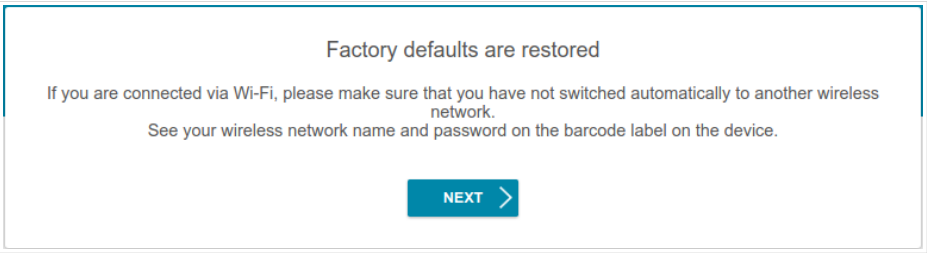
To start the Initial Configuration Wizard, go to the **Initial Configuration** section. On the opened page, click the **OK** button and wait until the factory default settings are restored.



In order to run the initial setup wizard, the device should be reset to factory defaults.

Figure 21. Restoring the default settings in the Wizard.

If you perform initial configuration of the router via Wi-Fi connection, please make sure that you are connected to the wireless network of DIR-853 (see the WLAN name (SSID) on the barcode label on the bottom panel of the device) and click the **NEXT** button.

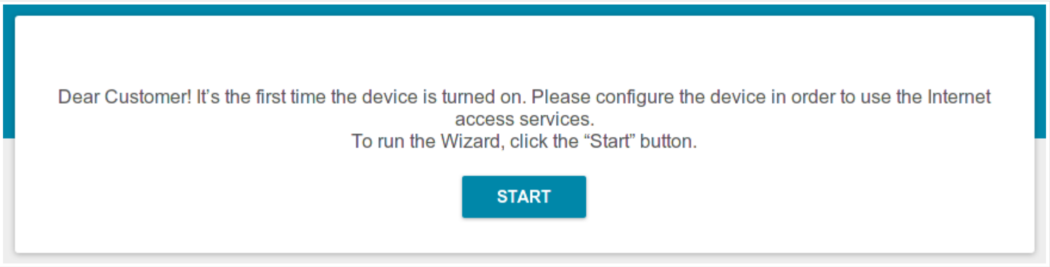


Factory defaults are restored

If you are connected via Wi-Fi, please make sure that you have not switched automatically to another wireless network.
See your wireless network name and password on the barcode label on the device.

Figure 22. Checking connection to the wireless network.

Click the **START** button.



Dear Customer! It's the first time the device is turned on. Please configure the device in order to use the Internet access services.
To run the Wizard, click the "Start" button.

Figure 23. Starting the Wizard.

On the opened page, click **YES** in order to leave the current language of the web-based interface or click **NO** to select the other language.

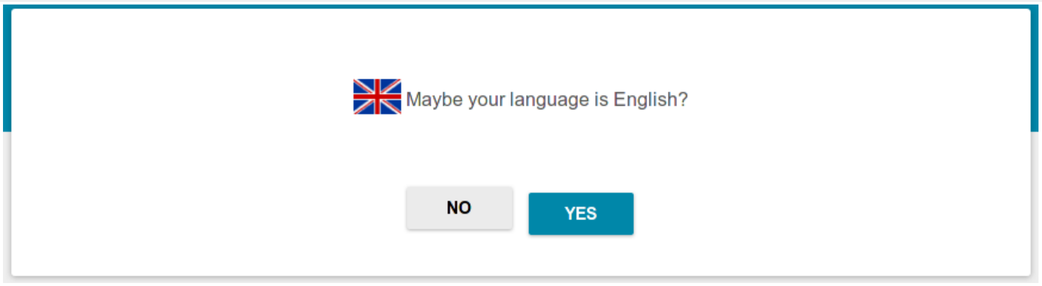
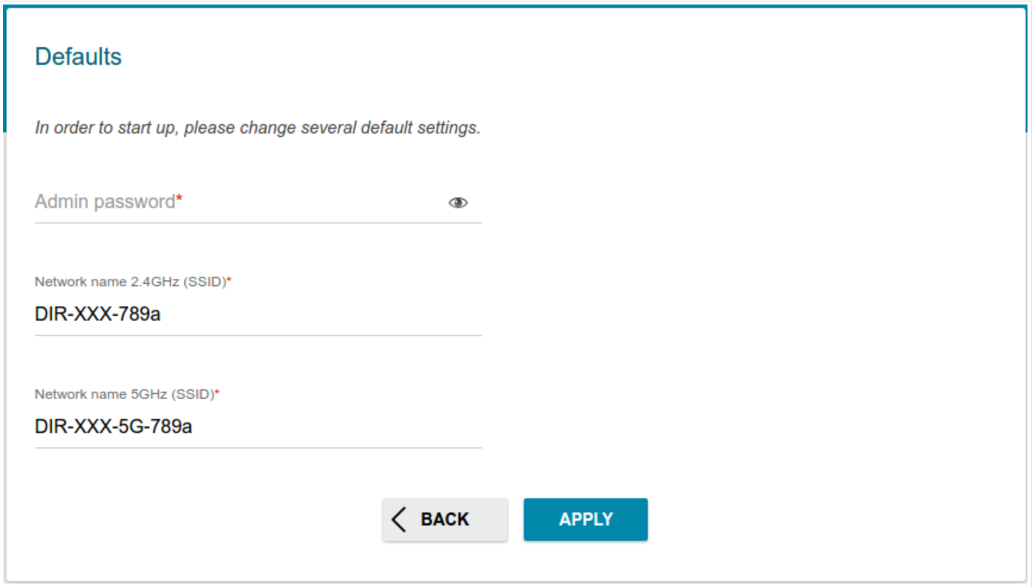

Maybe your language is English?

Figure 24. Selecting a language.

You can finish the wizard earlier and go to the menu of the web-based interface. To do this, click the **ADVANCED SETTINGS** button. On the opened page, change the default settings: specify the administrator password in the **Admin password** field and the name of the wireless network in the 2.4GHz and 5GHz bands in the **Network name 2.4GHz (SSID)** and **Network name 5GHz (SSID)** fields correspondingly. Then click the **APPLY** button.


Defaults

In order to start up, please change several default settings.

Admin password*

Network name 2.4GHz (SSID)*
DIR-XXX-789a

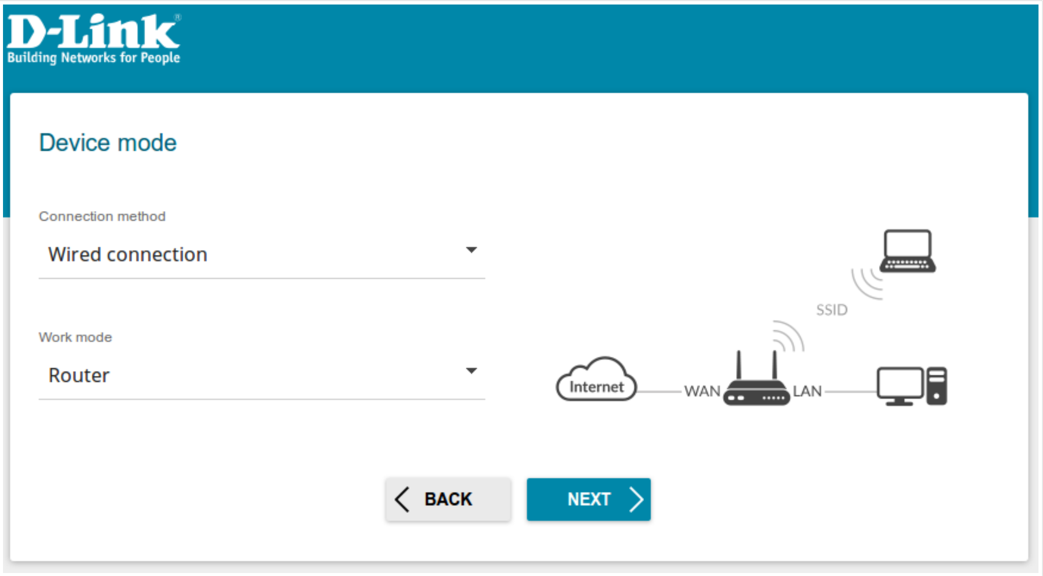
Network name 5GHz (SSID)*
DIR-XXX-5G-789a

Figure 25. Changing the default settings.

To continue the configuration of the router via the Wizard, click the **CONTINUE** button.

Selecting Operation Mode

In order to connect your device to a wired ISP, on the **Device mode** page, from the **Connection method** list, select the **Wired connection** value. Then from the **Work mode** list select the **Router** value. In this mode you can configure a WAN connection, set your own settings for the wireless network, configure LAN ports to connect an STB or VoIP phone, and set your own password for access to the web-based interface of the device.



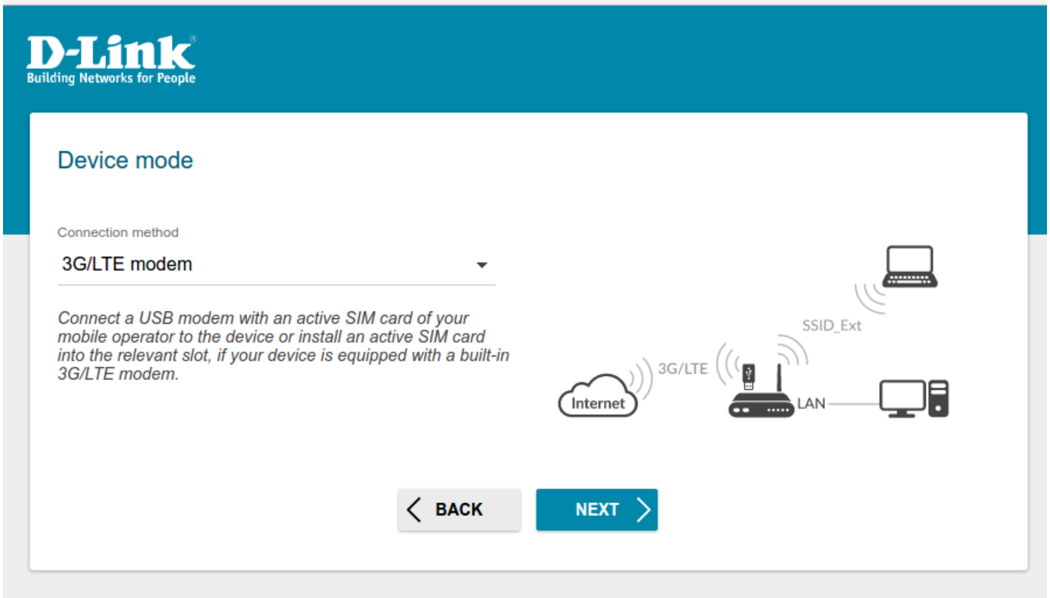
Device mode

Connection method: Wired connection

Work mode: Router

*Figure 26. Selecting an operation mode. The **Router** mode.*

In order to connect your device to the network of a 3G or LTE operator, on the **Device mode** page, from the **Connection method** list, select the **3G/LTE modem** value. In this mode you can configure a 3G/LTE WAN connection, set your own settings for the wireless network, and set your own password for access to the web-based interface of the device.



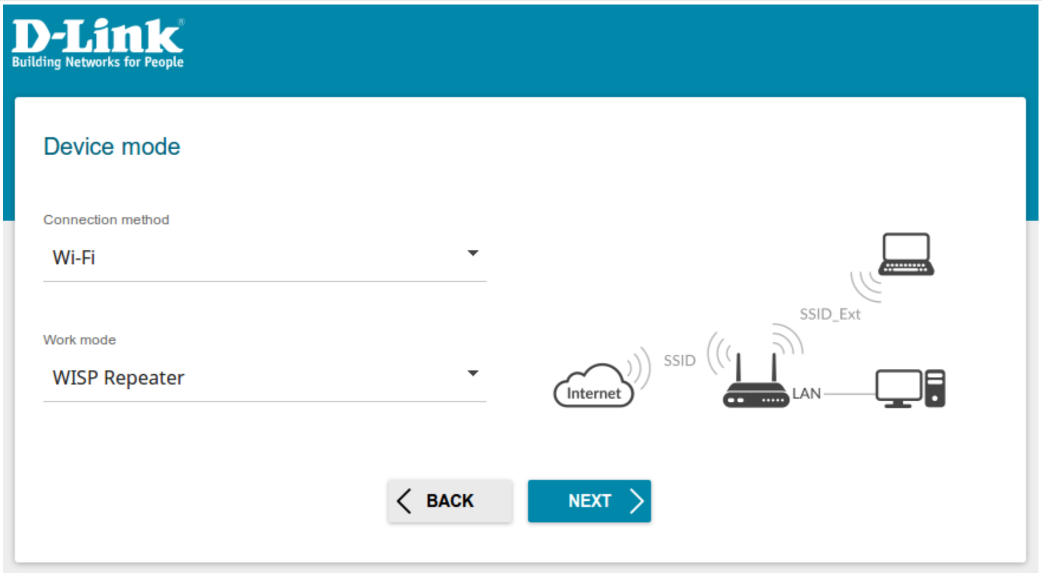
Device mode

Connection method: 3G/LTE modem

Connect a USB modem with an active SIM card of your mobile operator to the device or install an active SIM card into the relevant slot, if your device is equipped with a built-in 3G/LTE modem.

*Figure 27. Selecting an operation mode. The **3G/LTE modem** mode.*

In order to connect your device to a wireless ISP (WISP), on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **WISP Repeater** value. In this mode you can connect your device to another access point, configure a WAN connection, set your own settings for the wireless network, configure LAN ports to connect an STB or VoIP phone, and set your own password for access to the web-based interface of the device.



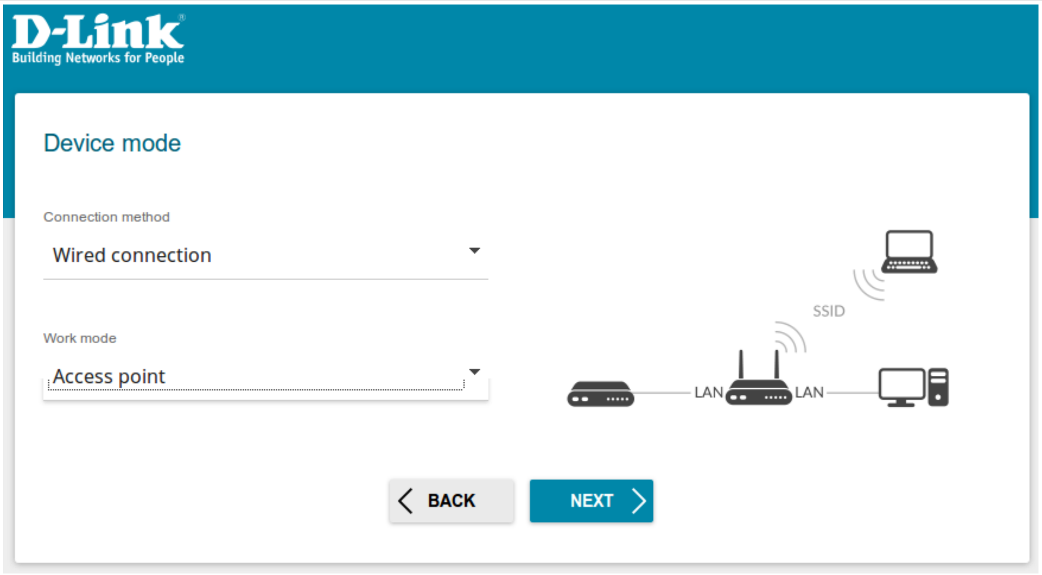
Device mode

Connection method: Wi-Fi

Work mode: WISP Repeater

*Figure 28. Selecting an operation mode. The **WISP Repeater** mode.*

In order to connect your device to a wired router for adding a wireless network to the existing local network, on the **Device mode** page, from the **Connection method** list, select the **Wired connection** value. Then from the **Work mode** list select the **Access point** value. In this mode you can change the LAN IP address, set your own settings for the wireless network and set your own password for access to the web-based interface of the device.



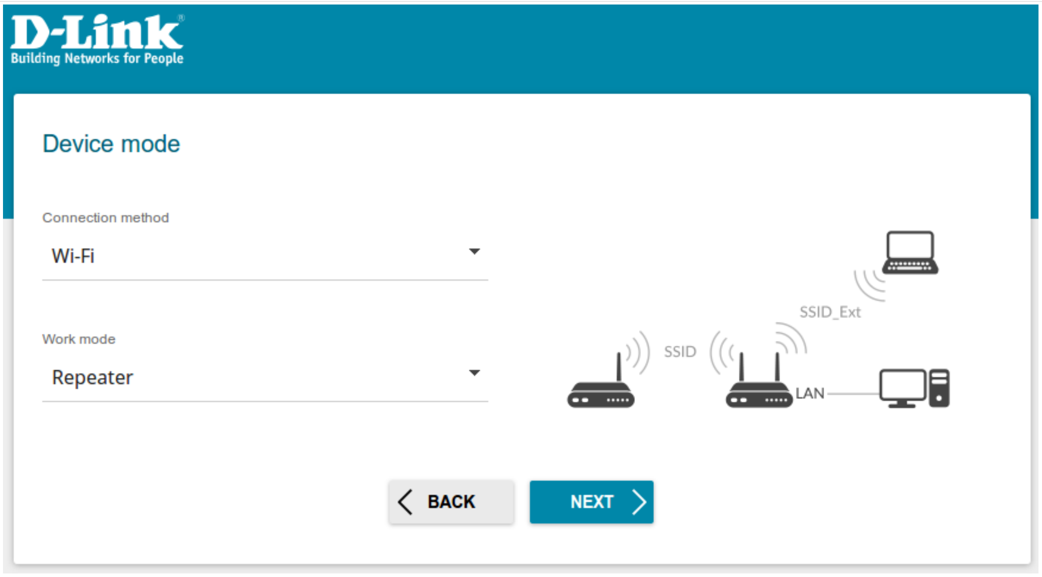
Device mode

Connection method: Wired connection

Work mode: Access point

*Figure 29. Selecting an operation mode. The **Access point** mode.*

In order to connect your device to a wireless router for extending the range of the existing wireless network, on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **Repeater** value. In this mode you can change the LAN IP address, connect your device to another access point, set your own settings for the wireless network, and set your own password for access to the web-based interface of the device.

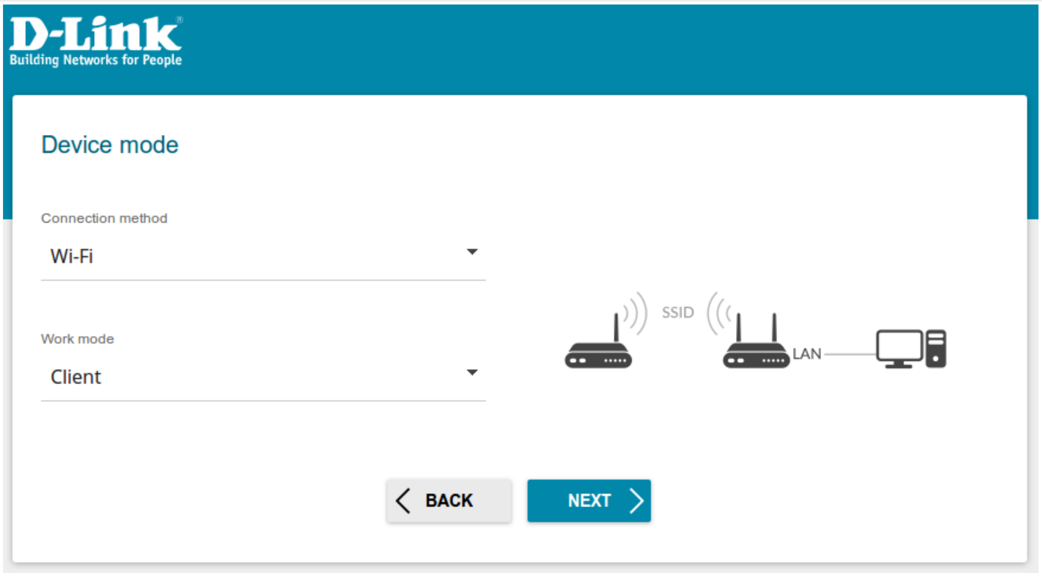

Device mode

Connection method: Wi-Fi

Work mode: Repeater

*Figure 30. Selecting an operation mode. The **Repeater** mode.*

In order to let wired PCs connected to your device access the network of a wireless router, on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **Client** value. In this mode you can change the LAN IP address, connect your device to another access point and set your own password for access to the web-based interface of the device.


Device mode

Connection method: Wi-Fi

Work mode: Client

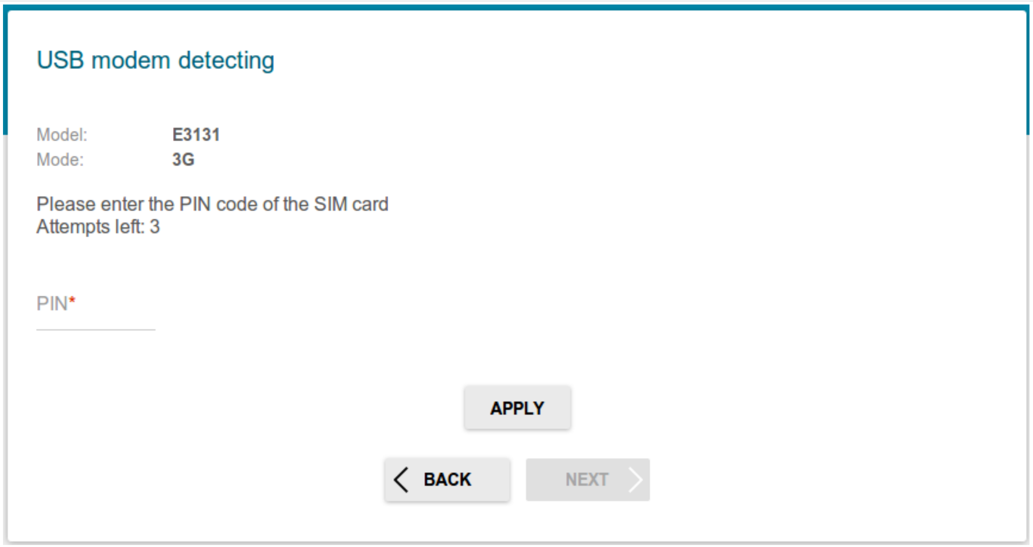
*Figure 31. Selecting an operation mode. The **Client** mode.*

When the operation mode is selected, click the **NEXT** button.

Creating 3G/LTE WAN Connection

This configuration step is available for the **3G/LTE modem** mode.

1. If the PIN code check is enabled for the SIM card inserted into your USB modem, enter the PIN code in the **PIN** field and click the **APPLY** button.



USB modem detecting

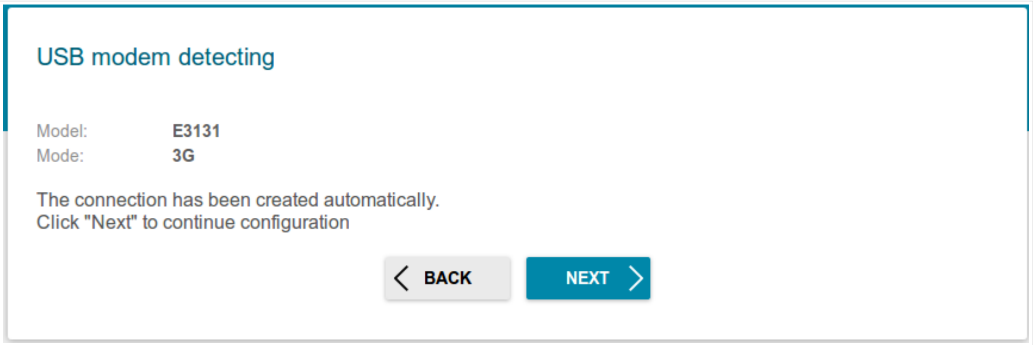
Model: E3131
Mode: 3G

Please enter the PIN code of the SIM card
Attempts left: 3

PIN*

Figure 32. The page for entering the PIN code.

2. Please wait while the router automatically creates a WAN connection for your mobile operator.



USB modem detecting

Model: E3131
Mode: 3G

The connection has been created automatically.
Click "Next" to continue configuration

Figure 33. The page for creating 3G/LTE connection.

3. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

If the router failed to create a WAN connection automatically, click the **CONFIGURE MANUALLY** button. On the **Internet connection type** page, configure all needed settings and click the **NEXT** button.

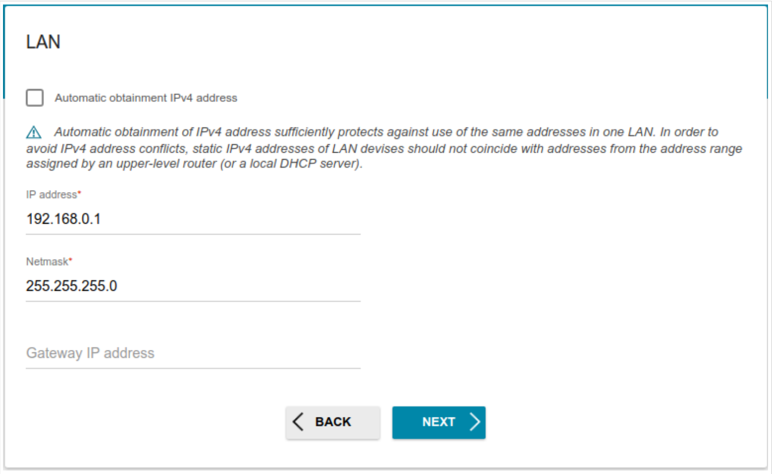
Changing LAN IPv4 Address

This configuration step is available for the **Access point**, **Repeater**, and **Client** modes.

1. Select the **Automatic obtainment of IPv4 address** to let DIR-853 automatically obtain the LAN IPv4 address.

> **!** If the router obtains the LAN IPv4 address automatically, then after finishing the Wizard you can access the web-based interface using the domain name (by default, `dlinkrouter.local`) with a dot at the end.

If you want to manually assign the LAN IPv4 address for DIR-853, do not select the **Automatic obtainment of IPv4 address** checkbox and fill in the **IP address** and **Netmask** fields and, if needed, the **Gateway IP address** field. Make sure that the assigned address does not coincide with the LAN IPv4 address of the router to which your device connects.



LAN

□ Automatic obtainment IPv4 address

⚠ *Automatic obtainment of IPv4 address sufficiently protects against use of the same addresses in one LAN. In order to avoid IPv4 address conflicts, static IPv4 addresses of LAN devises should not coincide with addresses from the address range assigned by an upper-level router (or a local DHCP server).*

IP address*
192.168.0.1

Netmask*
255.255.255.0

Gateway IP address

Figure 34. The page for changing the LAN IPv4 address.

2. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

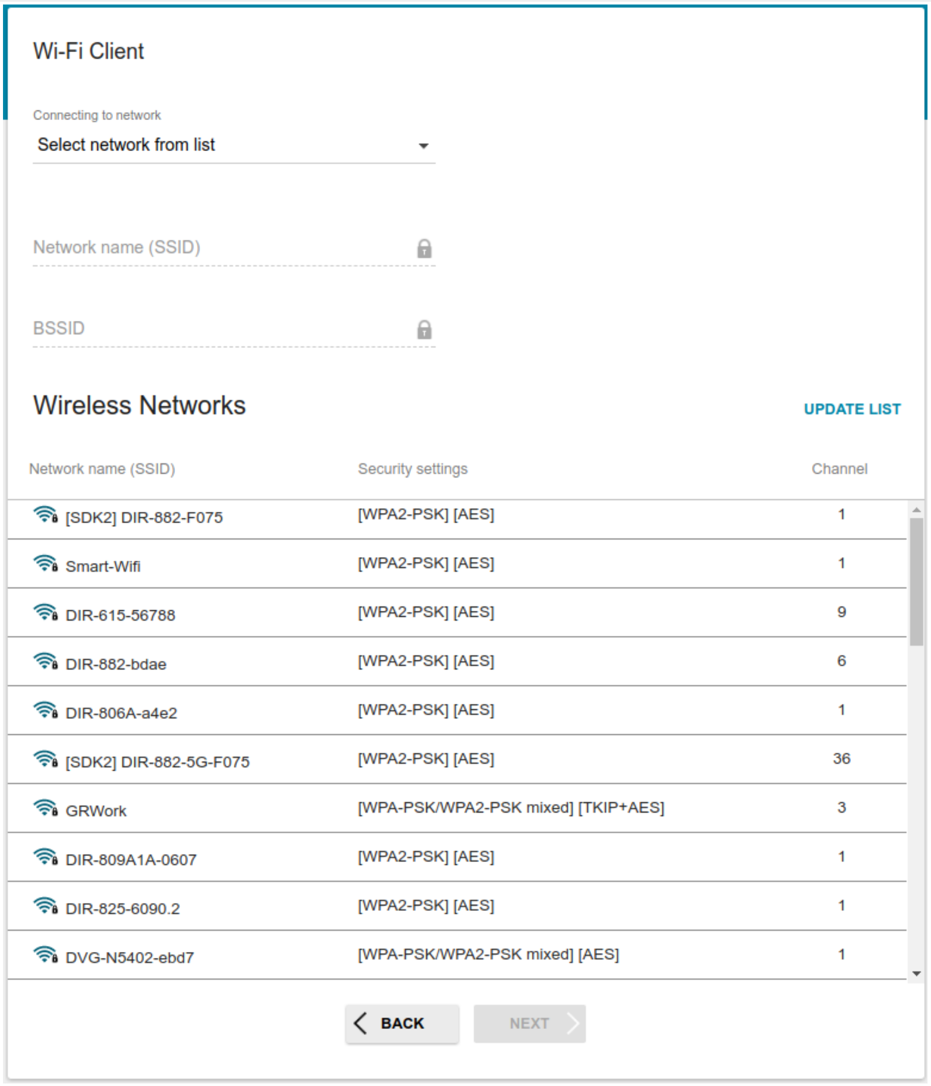
Wi-Fi Client

This configuration step is available for the **WISP Repeater**, **Repeater**, and **Client** modes.

1. On the **Wi-Fi Client** page, in the **Wireless Networks** section, select the network to which you want to connect. When you select a network, the **Network name (SSID)** and **BSSID** fields are filled in automatically.

If you cannot find the needed network in the list, click the **UPDATE LIST** button.

2. If a password is needed to connect to the selected network, fill in the relevant field.



Wi-Fi Client

Connecting to network: Select network from list

Network name (SSID)

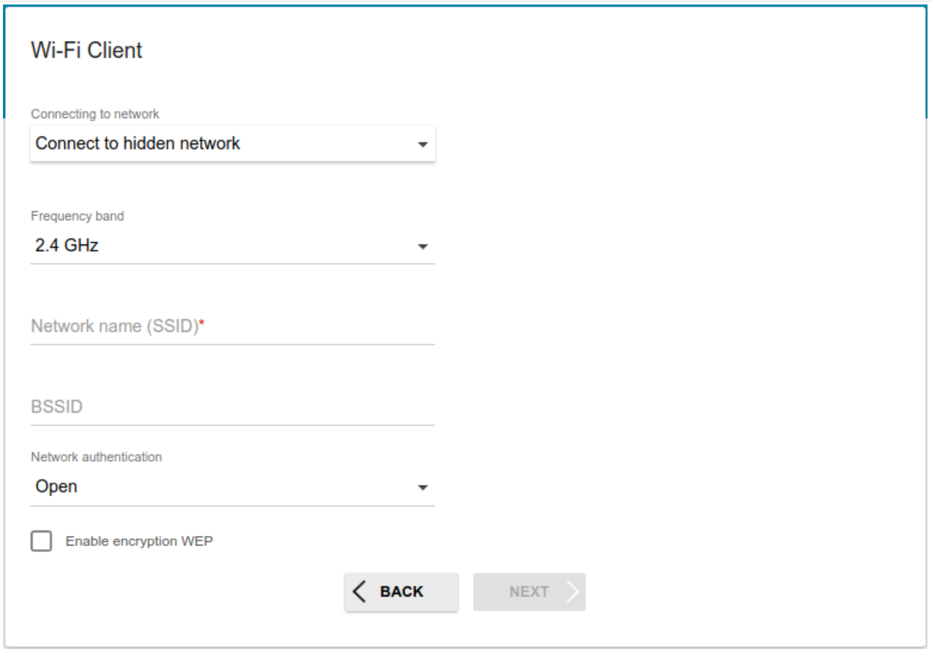
BSSID

Wireless Networks

Network name (SSID)	Security settings	Channel
[SDK2] DIR-882-F075	[WPA2-PSK] [AES]	1
Smart-Wifi	[WPA2-PSK] [AES]	1
DIR-615-56788	[WPA2-PSK] [AES]	9
DIR-882-bdae	[WPA2-PSK] [AES]	6
DIR-806A-a4e2	[WPA2-PSK] [AES]	1
[SDK2] DIR-882-5G-F075	[WPA2-PSK] [AES]	36
GRWork	[WPA-PSK/WPA2-PSK mixed] [TKIP+AES]	3
DIR-809A1A-0607	[WPA2-PSK] [AES]	1
DIR-825-6090.2	[WPA2-PSK] [AES]	1
DVG-N5402-ebd7	[WPA-PSK/WPA2-PSK mixed] [AES]	1

Figure 35. The page for configuring the Wi-Fi client.

If you connect to a hidden network, from the **Connecting to network** list select the **Connect to hidden network** value. Then select the band where the hidden network operates from the **Frequency band** list and enter the network name in the **Network name (SSID)** field. Then select a needed value from the **Network authentication** list and then, if needed, enter the password in the relevant field.



Wi-Fi Client

Connecting to network: Connect to hidden network

Frequency band: 2.4 GHz

Network name (SSID)*

BSSID

Network authentication: Open

□ Enable encryption WEP

Figure 36. The page for configuring connection to a hidden network.

3. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

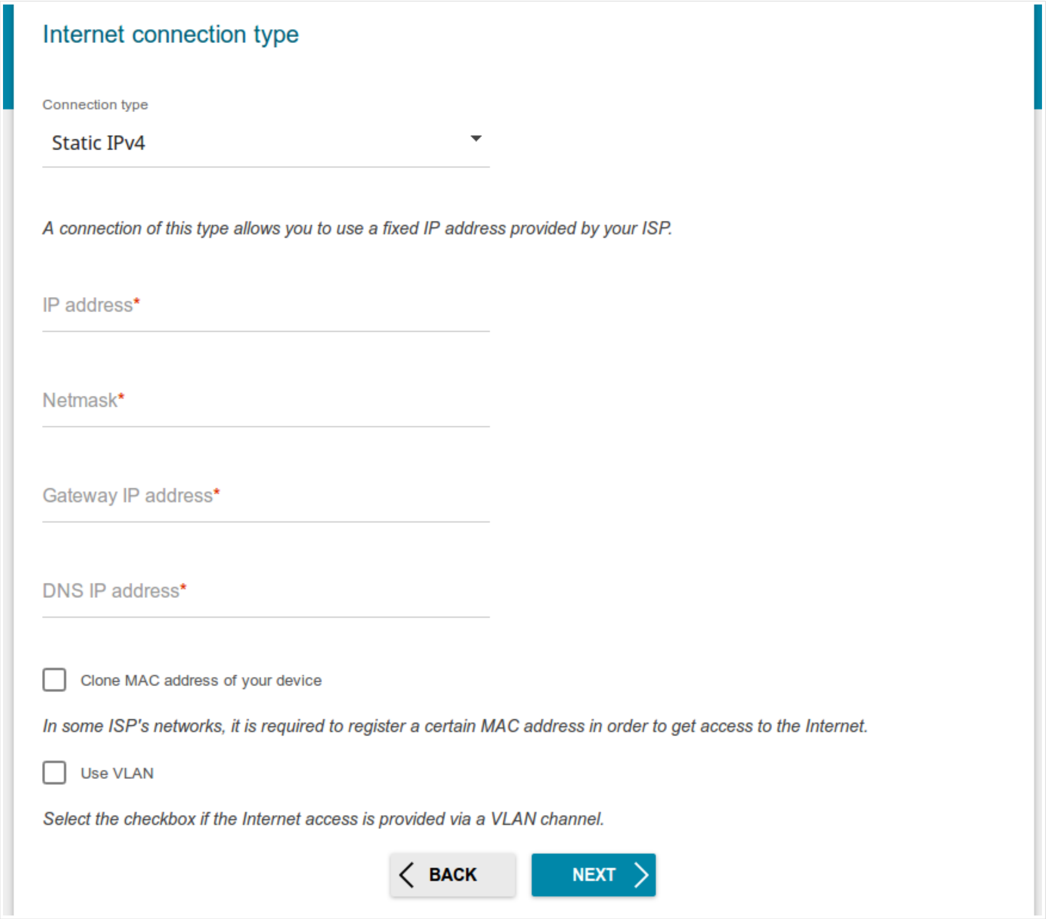
Creating WAN Connection

This configuration step is available for the **Router** and **WISP Repeater** modes.

! You should configure your WAN connection in accordance with data provided by your Internet service provider (ISP). Make sure that you have obtained all necessary information prior to configuring your connection. Otherwise contact your ISP.

1. On the **Internet connection type** page, from the **Connection type** list, select the connection type used by your ISP and fill in the fields displayed on the page.
2. Specify the settings necessary for the connection of the selected type.
3. If your ISP uses MAC address binding, select the **Clone MAC address of your device** checkbox.
4. If the Internet access is provided via a VLAN channel, select the **Use VLAN** checkbox and fill in the **VLAN ID** field.
5. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

Static IPv4 Connection



Internet connection type

Connection type
Static IPv4

A connection of this type allows you to use a fixed IP address provided by your ISP.

IP address*

Netmask*

Gateway IP address*

DNS IP address*

□ Clone MAC address of your device

In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet.

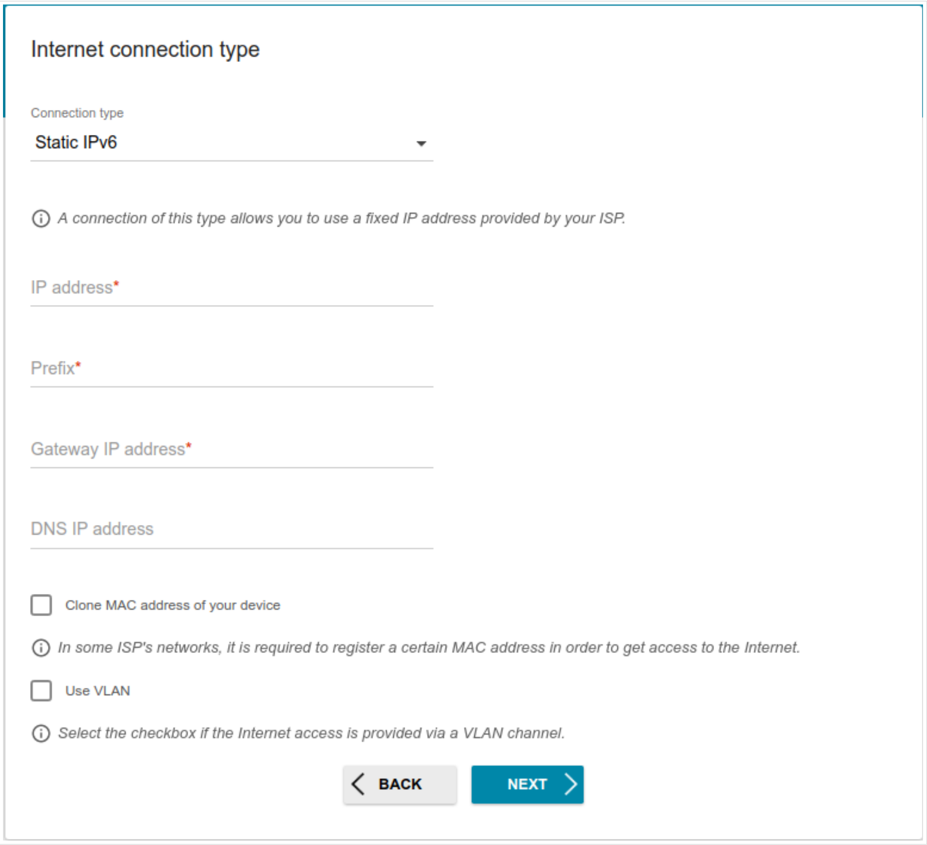
□ Use VLAN

Select the checkbox if the Internet access is provided via a VLAN channel.

Figure 37. The page for configuring Static IPv4 WAN connection.

Fill in the following fields: **IP address**, **Netmask**, **Gateway IP address**, and **DNS IP address**.

Static IPv6 Connection



Internet connection type

Connection type
Static IPv6

ⓘ *A connection of this type allows you to use a fixed IP address provided by your ISP.*

IP address*

Prefix*

Gateway IP address*

DNS IP address

□ Clone MAC address of your device

ⓘ *In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet.*

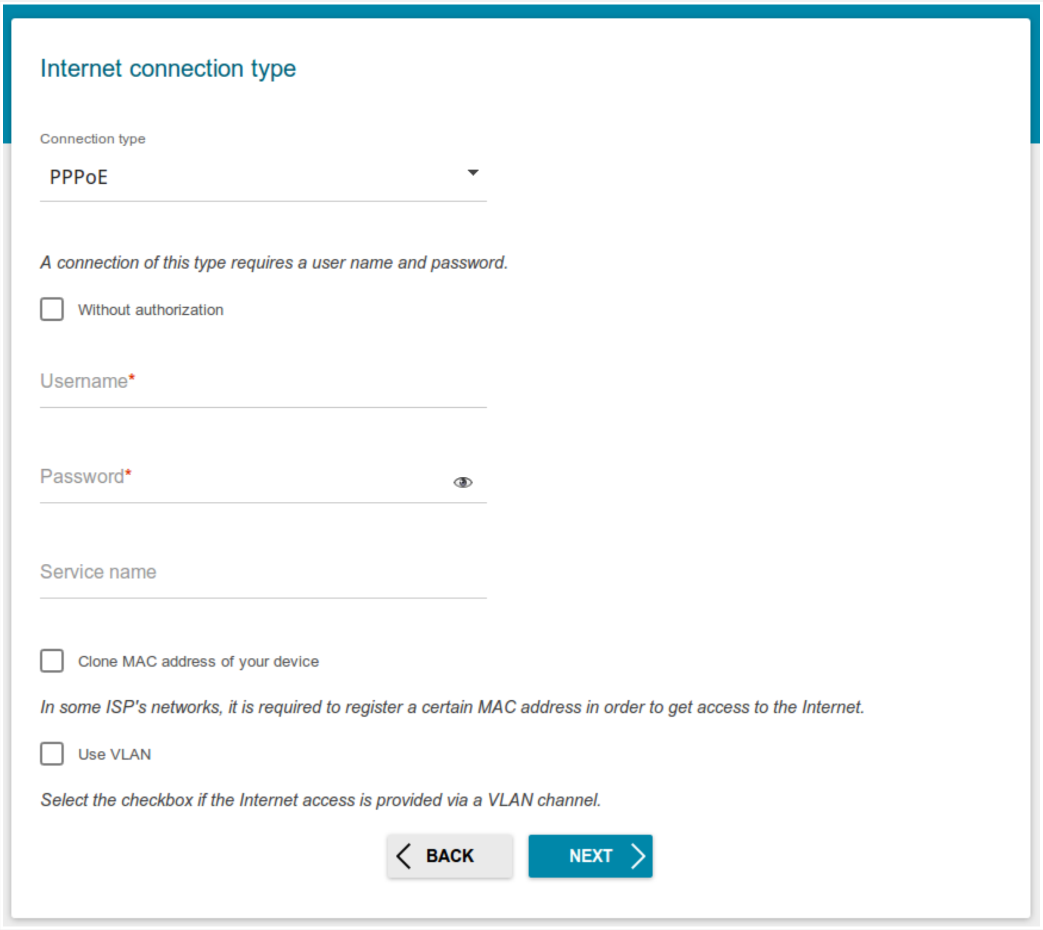
□ Use VLAN

ⓘ *Select the checkbox if the Internet access is provided via a VLAN channel.*

Figure 38. The page for configuring Static IPv6 WAN connection.

Fill in the following fields: **IP address**, **Prefix**, and **Gateway IP address**.

PPPoE, IPv6 PPPoE, PPPoE Dual Stack, PPPoE + Dynamic IP (PPPoE Dual Access) Connections



Internet connection type

Connection type: PPPoE

A connection of this type requires a user name and password.

□ Without authorization

Username*

Password*

Service name

□ Clone MAC address of your device

In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet.

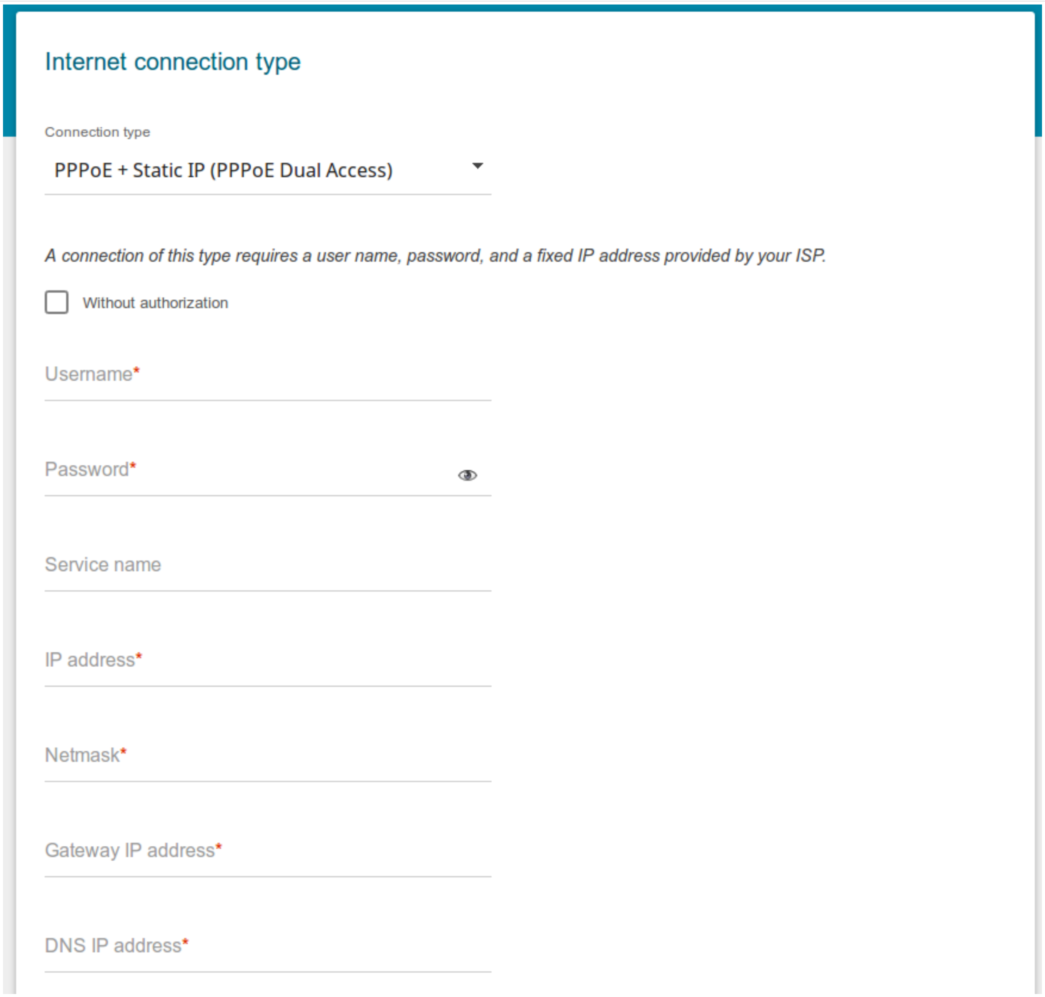
□ Use VLAN

Select the checkbox if the Internet access is provided via a VLAN channel.

Figure 39. The page for configuring PPPoE WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon (👁) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

PPPoE + Static IP (PPPoE Dual Access) Connection



Internet connection type

Connection type
PPPoE + Static IP (PPPoE Dual Access)

A connection of this type requires a user name, password, and a fixed IP address provided by your ISP.

□ Without authorization

Username*

Password*

Service name

IP address*

Netmask*

Gateway IP address*

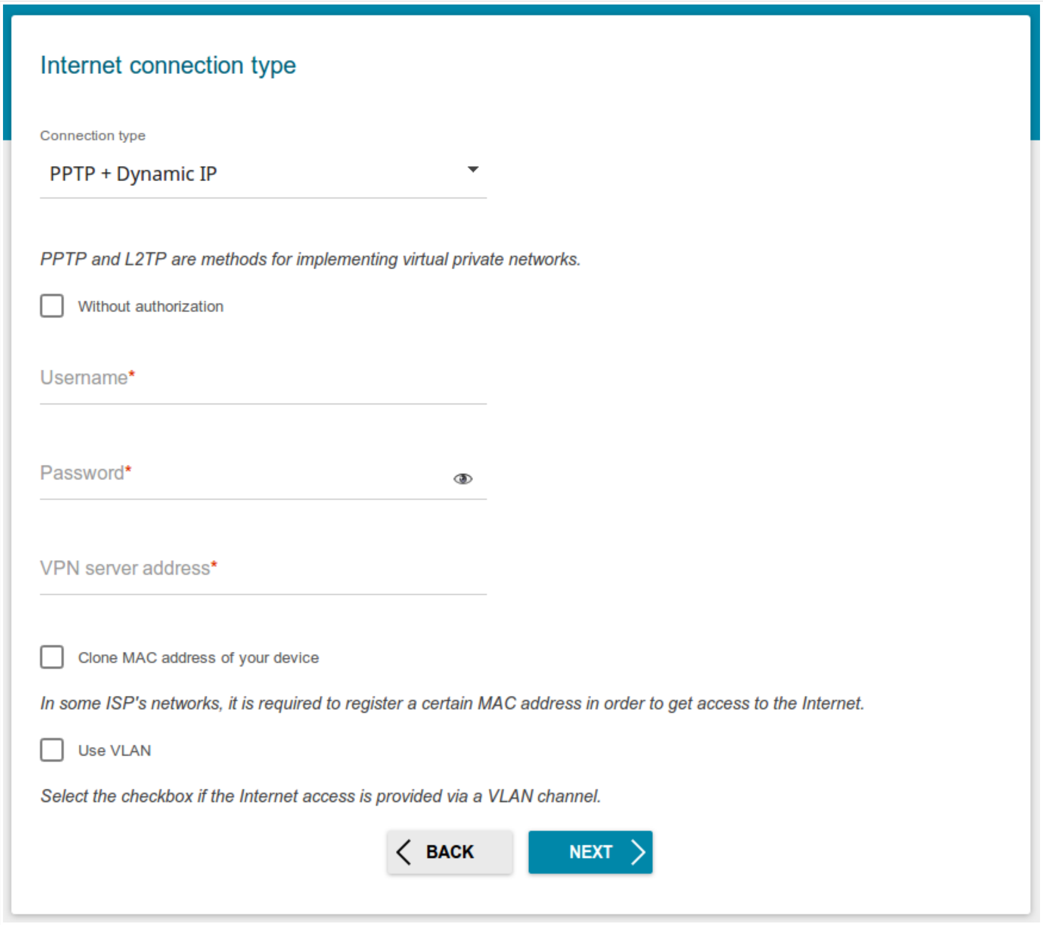
DNS IP address*

Figure 40. The page for configuring PPPoE + Static IP (PPPoE Dual Access) WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon (👁) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

Also fill in the following fields: **IP address**, **Netmask**, **Gateway IP address**, and **DNS IP address**.

PPTP + Dynamic IP or L2TP + Dynamic IP Connection



Internet connection type

Connection type
PPTP + Dynamic IP

PPTP and L2TP are methods for implementing virtual private networks.

□ Without authorization

Username*

Password*

VPN server address*

□ Clone MAC address of your device

In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet.

□ Use VLAN

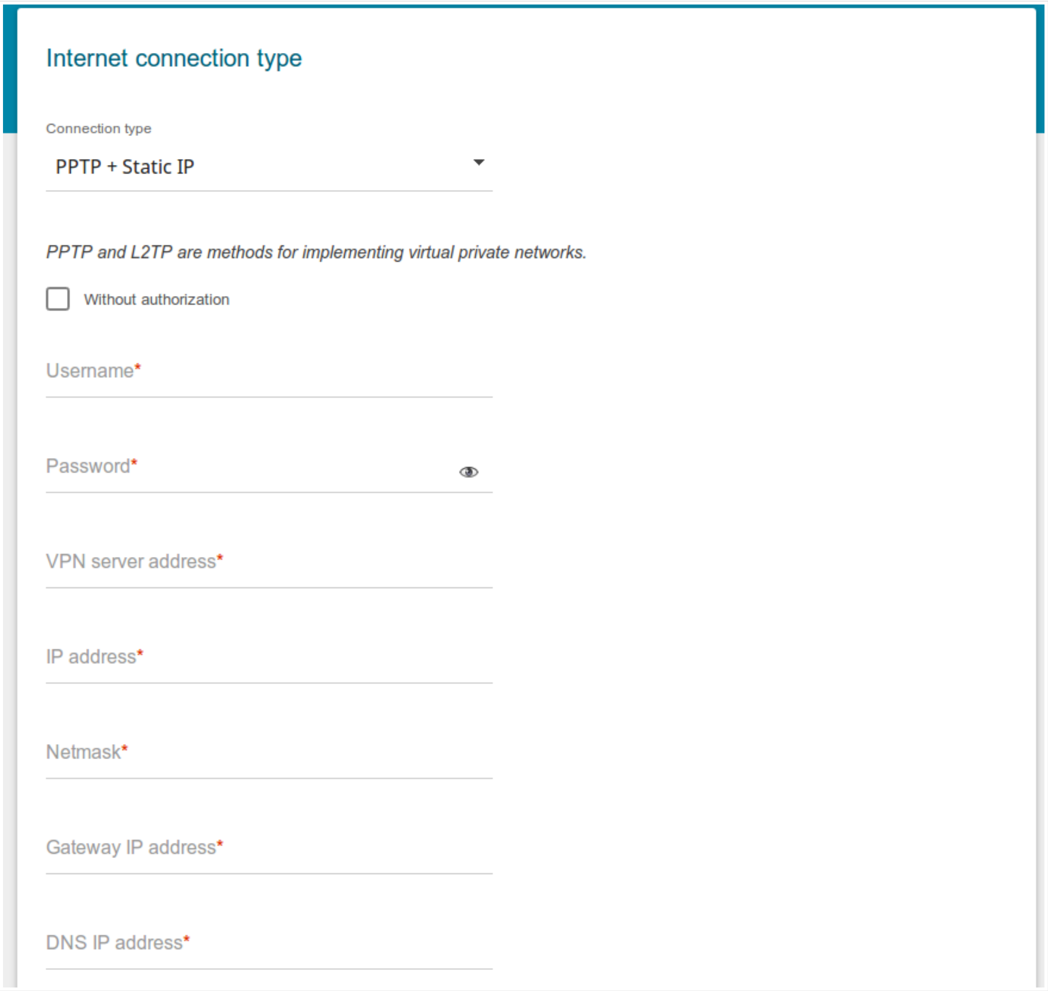
Select the checkbox if the Internet access is provided via a VLAN channel.

Figure 41. The page for configuring PPTP + Dynamic IP WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon (👁) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

In the **VPN server address** field, enter the IP or URL address of the PPTP or L2TP authentication server.

PPTP + Static IP or L2TP + Static IP Connection



Internet connection type

Connection type
PPTP + Static IP

PPTP and L2TP are methods for implementing virtual private networks.

□ Without authorization

Username*

Password*

VPN server address*

IP address*

Netmask*

Gateway IP address*

DNS IP address*

Figure 42. The page for configuring PPTP + Static IP WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon (👁) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

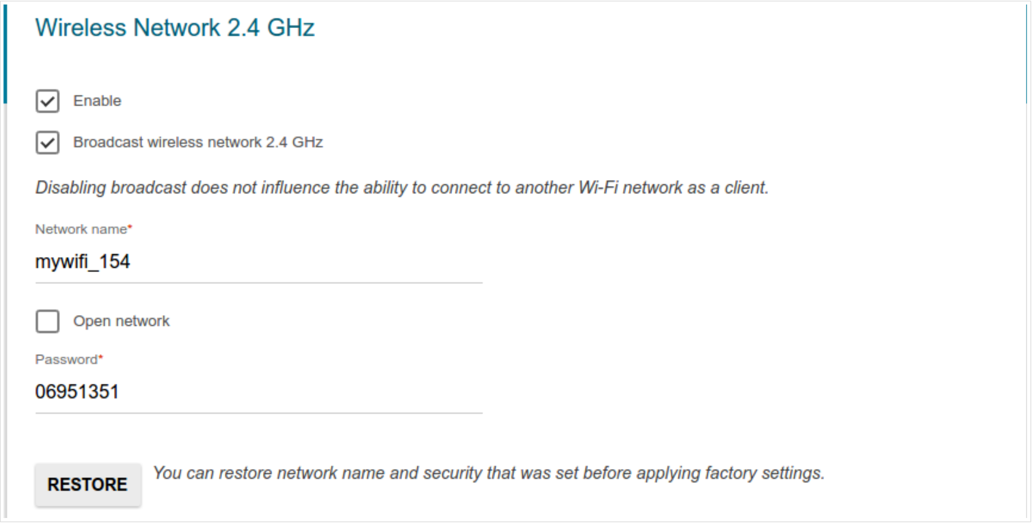
In the **VPN server address** field, enter the IP or URL address of the PPTP or L2TP authentication server.

Also fill in the following fields: **IP address**, **Netmask**, **Gateway IP address**, and **DNS IP address**.

Configuring Wireless Network

This configuration step is available for the **3G/LTE modem**, **Router**, **Access point**, **WISP Repeater**, and **Repeater** modes.

1. On the **Wireless Network 2.4 GHz** page, in the **Network name** field, specify your own name for the wireless network or leave the value suggested by the router.
2. In the **Password** field, specify your own password for access to the wireless network or leave the value suggested by the router (WPS PIN of the device, see the barcode label).
3. You can restore the parameters of the wireless network specified before resetting to factory defaults. To do this, click the **RESTORE** button.



Wireless Network 2.4 GHz

☑ Enable

☑ Broadcast wireless network 2.4 GHz

Disabling broadcast does not influence the ability to connect to another Wi-Fi network as a client.

Network name*
mywifi_154

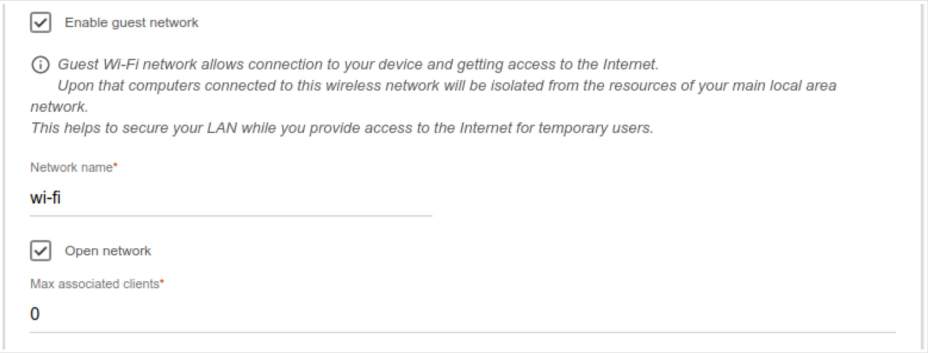
□ Open network

Password*
06951351

You can restore network name and security that was set before applying factory settings.

Figure 43. The page for configuring the wireless network.

4. If you want to create an additional wireless network isolated from your LAN, select the **Enable guest network** checkbox (available for the **3G/LTE modem**, **Router**, and **WISP Repeater** modes only).



☑ Enable guest network

ⓘ *Guest Wi-Fi network allows connection to your device and getting access to the Internet.*
Upon that computers connected to this wireless network will be isolated from the resources of your main local area network.
This helps to secure your LAN while you provide access to the Internet for temporary users.

Network name*
wi-fi

☑ Open network

Max associated clients*
0

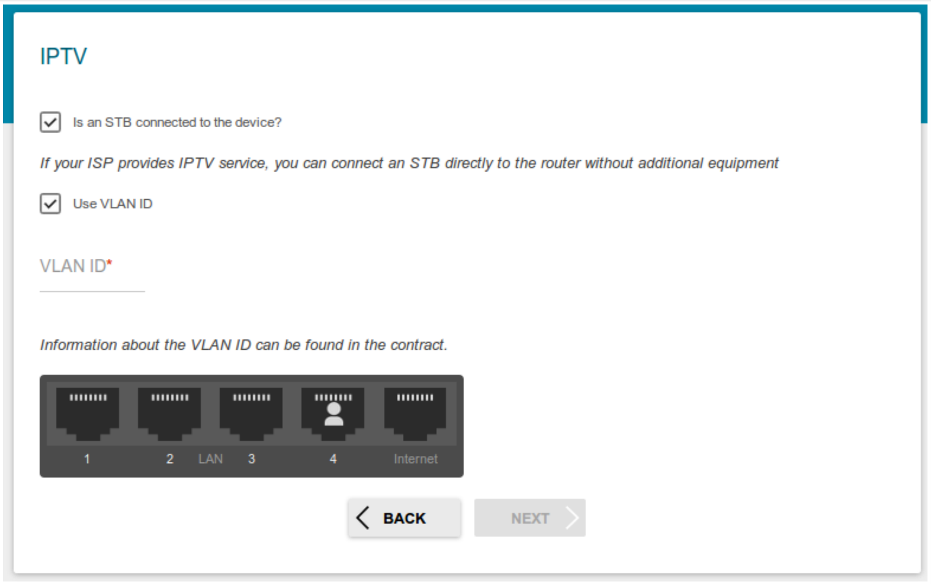
Figure 44. The page for configuring the wireless network.

5. In the **Network name** field, specify your own name for the guest wireless network or leave the value suggested by the router.
6. If you want to create a password for access to the guest wireless network, deselect the **Open network** checkbox and fill in the **Password** field.
7. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.
8. On the **Wireless Network 5 GHz** page, specify needed settings for the wireless network in the 5GHz band and click the **NEXT** button.

Configuring LAN Ports for IPTV/VoIP

This configuration step is available for the **Router** and **WISP Repeater** modes.

1. On the **IPTV** page, select the **Is an STB connected to the device** checkbox.



IPTV

☑ Is an STB connected to the device?

If your ISP provides IPTV service, you can connect an STB directly to the router without additional equipment

☑ Use VLAN ID

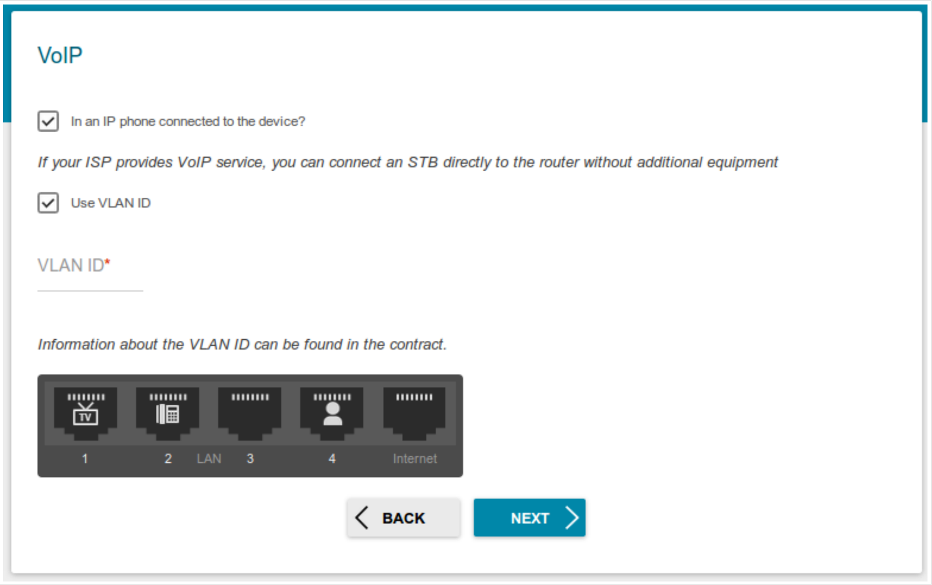
VLAN ID*

Information about the VLAN ID can be found in the contract.

Figure 45. The page for selecting a LAN port to connect an IPTV set-top box.

2. Select a free LAN port for connecting your set-top box.
3. If the IPTV service is provided via a VLAN channel, select the **Use VLAN ID** checkbox and fill in the **VLAN ID** field.
4. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.

5. On the **VoIP** page, select the **In an IP phone connected to the device** checkbox.



VoIP

☑ In an IP phone connected to the device?

If your ISP provides VoIP service, you can connect an STB directly to the router without additional equipment

☑ Use VLAN ID

VLAN ID*

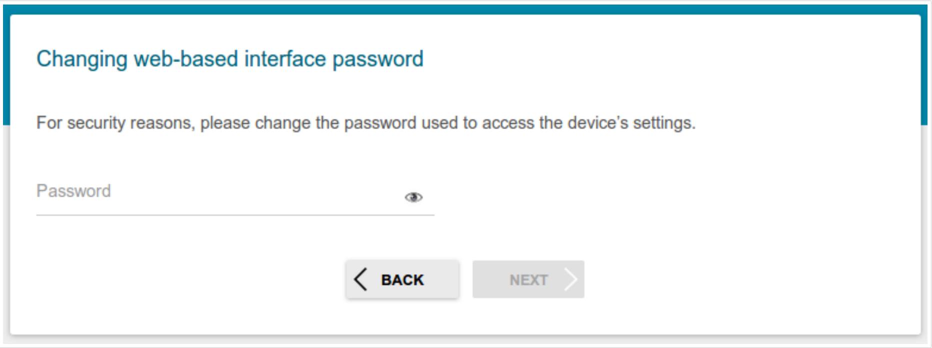
Information about the VLAN ID can be found in the contract.

Figure 46. The page for selecting a LAN port to connect an VoIP phone.

6. Select a free LAN port for connecting your IP phone.
7. If the VoIP service is provided via a VLAN channel, select the **Use VLAN ID** checkbox and fill in the **VLAN ID** field.
8. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.

Changing Web-based Interface Password

On this page, you should change the default administrator password. You may set any password except **admin**. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[9]



Changing web-based interface password

For security reasons, please change the password used to access the device's settings.

Password

Figure 47. The page for changing the web-based interface password.

! Remember or write down the new password for the administrator account. In case of losing the new password, you can access the settings of the router only after restoring the factory default settings via the hardware **RESET** button. This procedure wipes out all settings that you have configured for your router.

Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

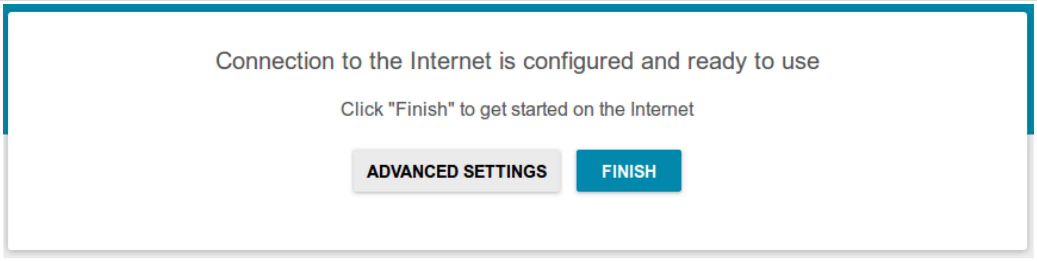
On the next page, check all specified settings.

Also you can save a text file with parameters set by the Wizard to your PC. To do this, click the **SAVE CONFIGURATION FILE** button and follow the dialog box appeared.

To finish the Wizard, click the **APPLY** button. The router will apply settings and reboot. Click the **BACK** button to specify other settings.

[9] 0-9, A-Z, a-z, space, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

If the Wizard has configured a WAN connection, after clicking the **APPLY** button, the page for checking the Internet availability opens.



Connection to the Internet is configured and ready to use

Click "Finish" to get started on the Internet

Figure 48. Checking the Internet availability.

If the router has been successfully connected to the Internet, click the **FINISH** button.

If problems appeared when connecting to the Internet, click the **CHECK AGAIN** button to recheck the state of the WAN connection.

If problems of connection have not been solved, contact the technical support of your ISP (as a rule, the technical support phone is provided with the agreement) or the D-Link technical support (the phone number will be displayed on the page after several attempts of checking the connection).

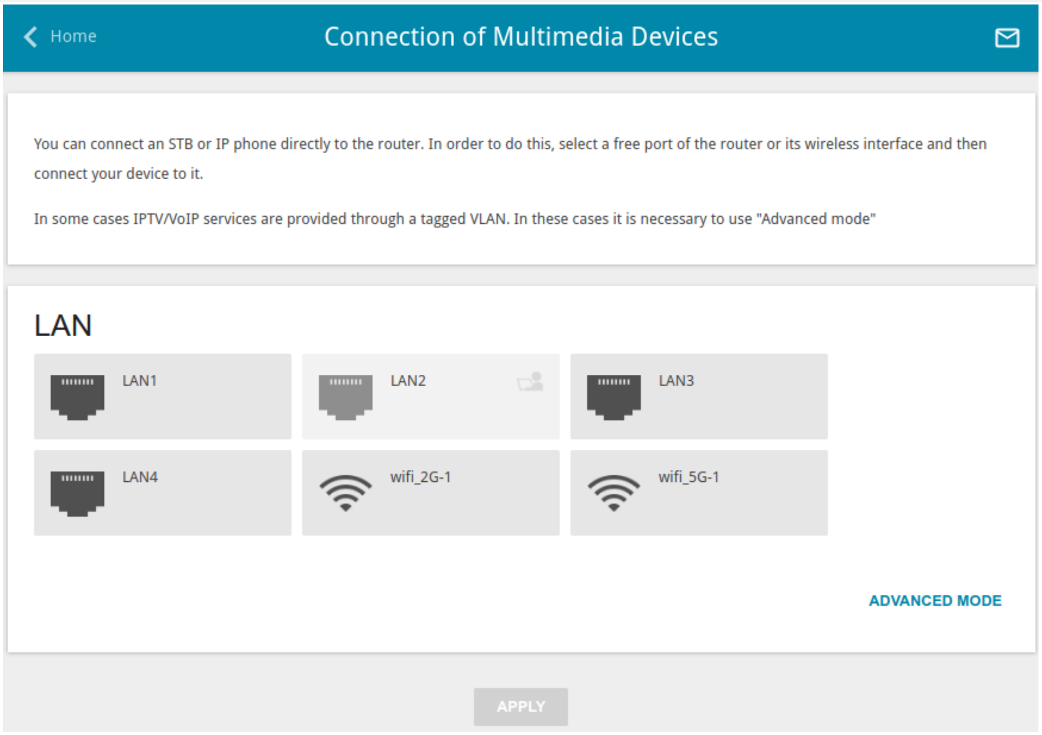
To specify other settings, click the **ADVANCED SETTINGS** button. After clicking the **ADVANCED SETTINGS** button, the **Home** page opens (see the ***Home Page*** section, page 38).

Connection of Multimedia Devices

The Multimedia Devices Connection Wizard helps to configure LAN ports or available wireless interfaces of the router for connecting additional devices, for example, an IPTV set-top box or IP phone. Contact your ISP to clarify if you need to configure DIR-853 in order to use these devices.

To start the Wizard, on the **Home** page, select the **Connection of Multimedia Devices** section.

If you need to select a port or wireless interface in order to use an additional device, left-click the relevant element in the **LAN** section (the selected element will be marked with a frame). Then click the **APPLY** button.



You can connect an STB or IP phone directly to the router. In order to do this, select a free port of the router or its wireless interface and then connect your device to it.

In some cases IPTV/VoIP services are provided through a tagged VLAN. In these cases it is necessary to use "Advanced mode"

Figure 49. The Multimedia Devices Connection Wizard. The simple mode.

If you need to configure a connection via VLAN, click the **ADVANCED MODE** button.

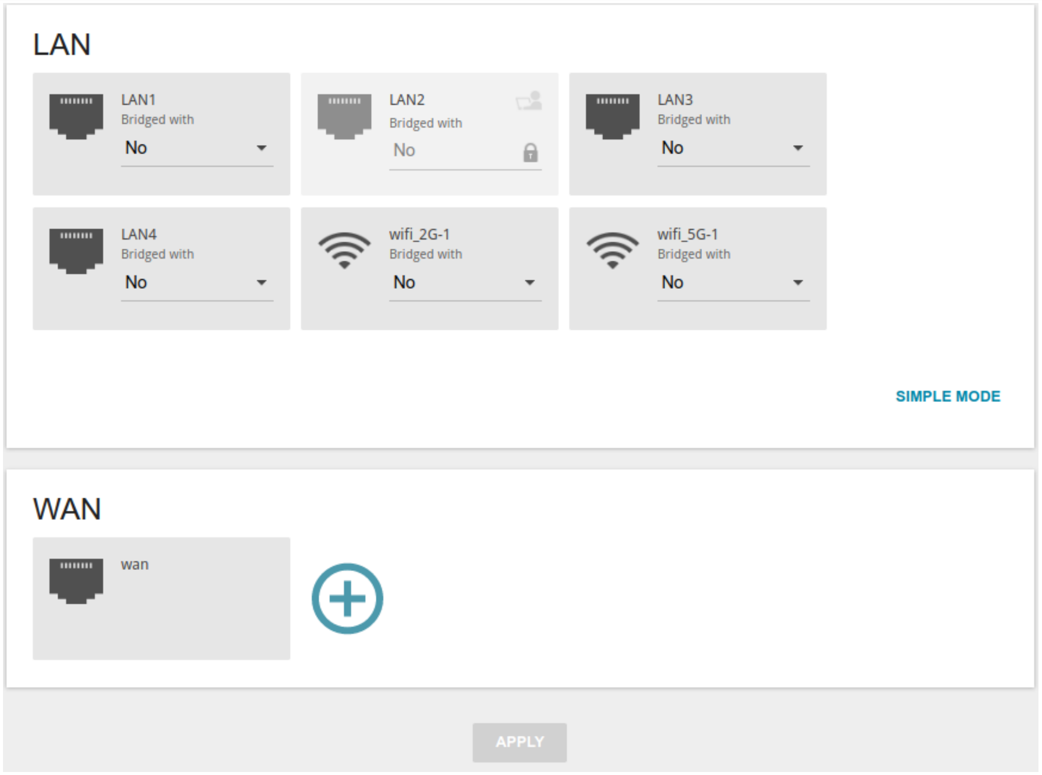


Figure 50. The Multimedia Devices Connection Wizard. The advanced mode.

In the **WAN** section, click the **Add** icon (⊕).

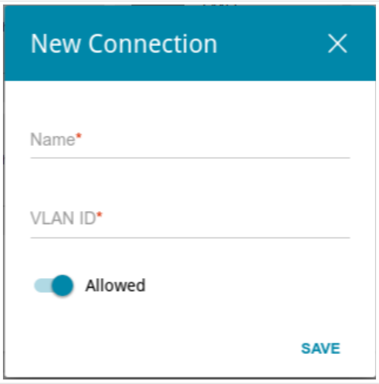


Figure 51. Adding a connection.

In the opened window, specify a name of the connection for easier identification in the **Name** field (you can specify any name). Specify the VLAN ID provided by your ISP and click the **SAVE** button.

Then in the **LAN** section, from the **Bridged with** drop-down list of the element corresponding to the LAN port or wireless interface to which the additional device is connected, select the created connection. Click the **APPLY** button.

! The selected port or wireless interface cannot use the default connection to access the Internet.

To deselect the port or wireless interface in the simple mode, left-click the selected element (the frame will disappear) and click the **APPLY** button.

To deselect the port or wireless interface in the advanced mode, select the **No** value from the **Bridged with** drop-down list of the element corresponding to the needed LAN port or interface. Then in the **WAN** section, select the connection via VLAN which will not be used any longer and click the **REMOVE** button. Then click the **APPLY** button.

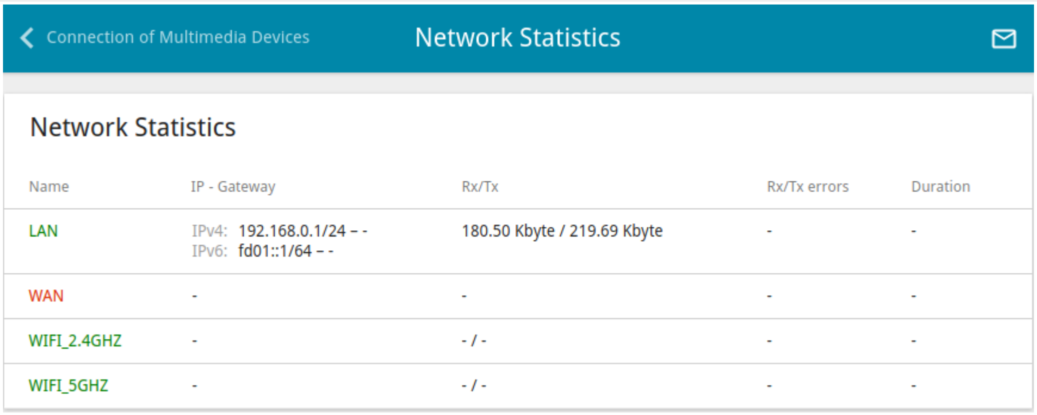
Statistics

The pages of this section display data on the current state of the router:

- network statistics
- IP addresses leased by the DHCP server
- the routing table
- data on devices connected to the router's network and its web-based interface
- addresses of active multicast groups
- active sessions.

Network Statistics

On the **Statistics / Network Statistics** page, you can view statistics for all connections existing in the system (WAN connections, LAN, WLAN). For each connection the following data are displayed: name and state (when the connection is on, its name is highlighted in green, when the connection is off, its name is highlighted in red), IP address and subnet mask, gateway (if the connection is established), MAC address, and volume of data received and transmitted (with increase of the volume the units of measurement are changed automatically: byte, Kbyte, Mbyte, Gbyte).



Network Statistics

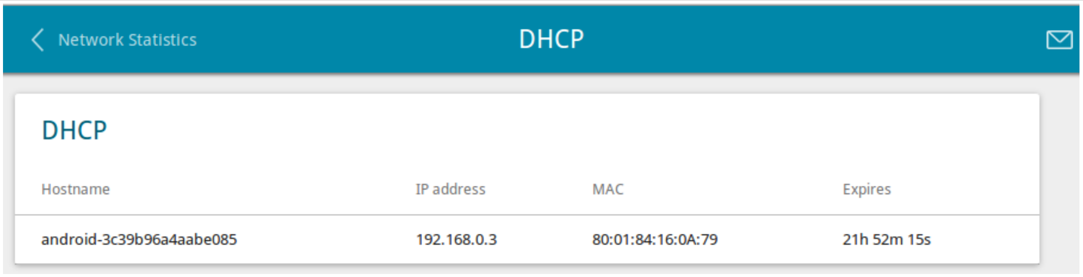
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.1/24 – - IPv6: fd01::1/64 – -	180.50 Kbyte / 219.69 Kbyte	-	-
WAN	-	-	-	-
WIFI_2.4GHZ	-	- / -	-	-
WIFI_5GHZ	-	- / -	-	-

*Figure 52. The **Statistics / Network Statistics** page.*

To view data on a connection, click the line corresponding to this connection.

DHCP

The **Statistics / DHCP** page displays the information on computers that have been identified by hostnames and MAC addresses and have got IP addresses from the DHCP server of the device, as well as the IP address expiration periods (the lease time).



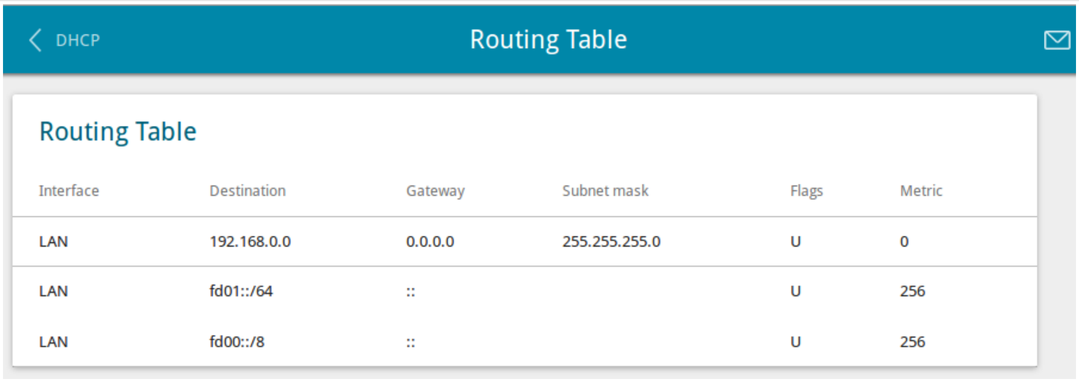
DHCP

Hostname	IP address	MAC	Expires
android-3c39b96a4aabe085	192.168.0.3	80:01:84:16:0A:79	21h 52m 15s

*Figure 53. The **Statistics / DHCP** page.*

Routing Table

The **Statistics / Routing Table** page displays the information on routes. The table contains destination IP addresses, gateways, subnet masks, and other data.



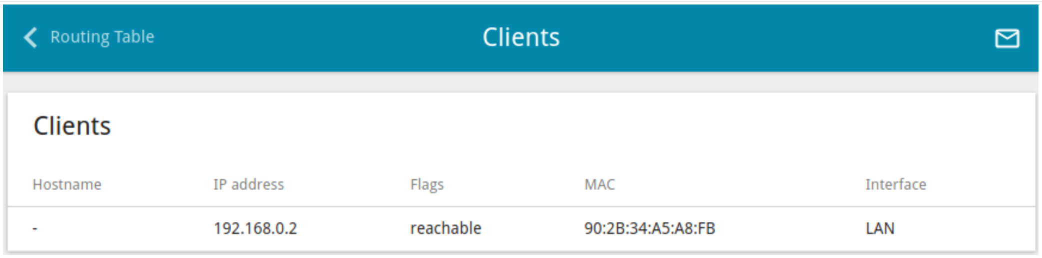
Routing Table

Interface	Destination	Gateway	Subnet mask	Flags	Metric
LAN	192.168.0.0	0.0.0.0	255.255.255.0	U	0
LAN	fd01::/64	::		U	256
LAN	fd00::/8	::		U	256

Figure 54. The ***Statistics / Routing Table*** *page.*

Clients

On the **Statistics / Clients** page, you can view the list of devices connected to the local network of the router.



Clients

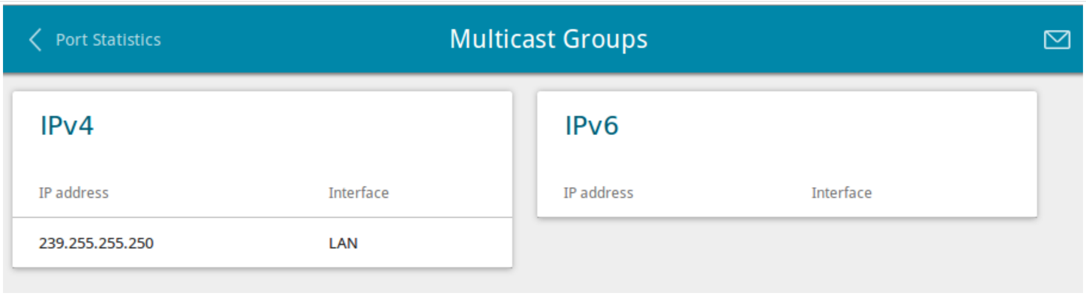
Hostname	IP address	Flags	MAC	Interface
-	192.168.0.2	reachable	90:2B:34:A5:A8:FB	LAN

*Figure 55. The **Statistics / Clients** page.*

For each device the following data are displayed: the IP address, the MAC address, and the network interface to which the device is connected.

Multicast Groups

The **Statistics / Multicast Groups** page displays addresses of active multicast groups (including IPTV channels and groups for transferring service information) to which the device is subscribed, and the interface through which the device is subscribed.



IPv4

IP address	Interface
239.255.255.250	LAN

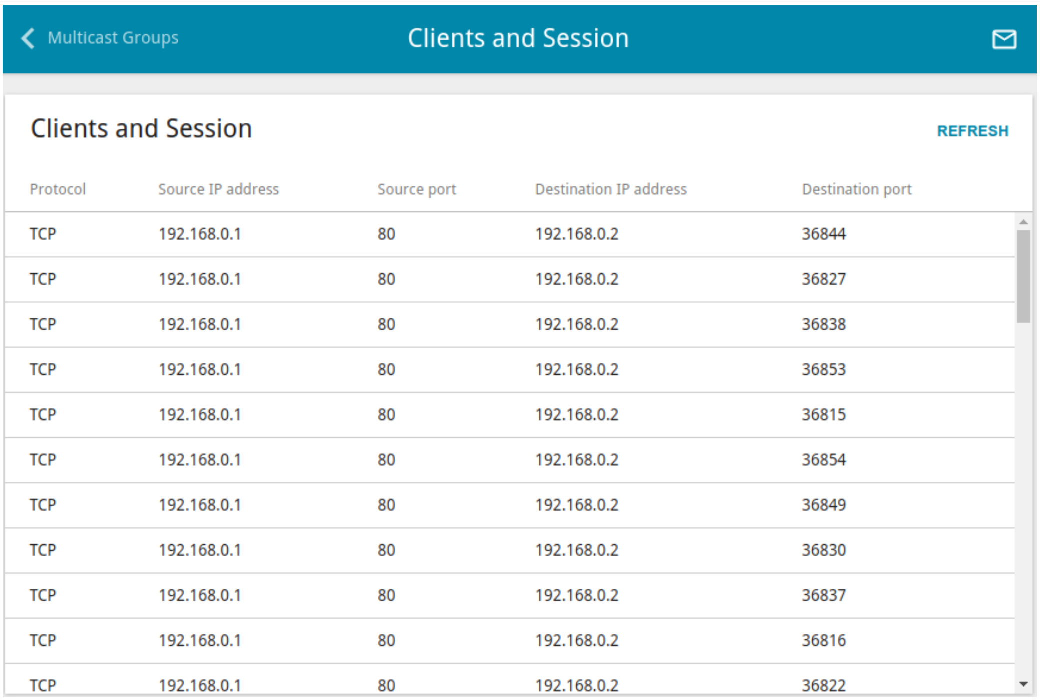
IPv6

IP address	Interface

*Figure 56. The **Statistics / Multicast Groups** page.*

Clients and Session

On the **Statistics / Clients and Session** page, you can view information on current sessions in the router's network. For each session the following data are displayed: the protocol for network packet transmission, the source IP address and port, and the destination IP address and port.



Clients and Session

REFRESH

Protocol	Source IP address	Source port	Destination IP address	Destination port
TCP	192.168.0.1	80	192.168.0.2	36844
TCP	192.168.0.1	80	192.168.0.2	36827
TCP	192.168.0.1	80	192.168.0.2	36838
TCP	192.168.0.1	80	192.168.0.2	36853
TCP	192.168.0.1	80	192.168.0.2	36815
TCP	192.168.0.1	80	192.168.0.2	36854
TCP	192.168.0.1	80	192.168.0.2	36849
TCP	192.168.0.1	80	192.168.0.2	36830
TCP	192.168.0.1	80	192.168.0.2	36837
TCP	192.168.0.1	80	192.168.0.2	36816
TCP	192.168.0.1	80	192.168.0.2	36822

*Figure 57. The **Statistics / Clients and Session** page.*

To view the latest data on current sessions in the router's network, click the **REFRESH** button.

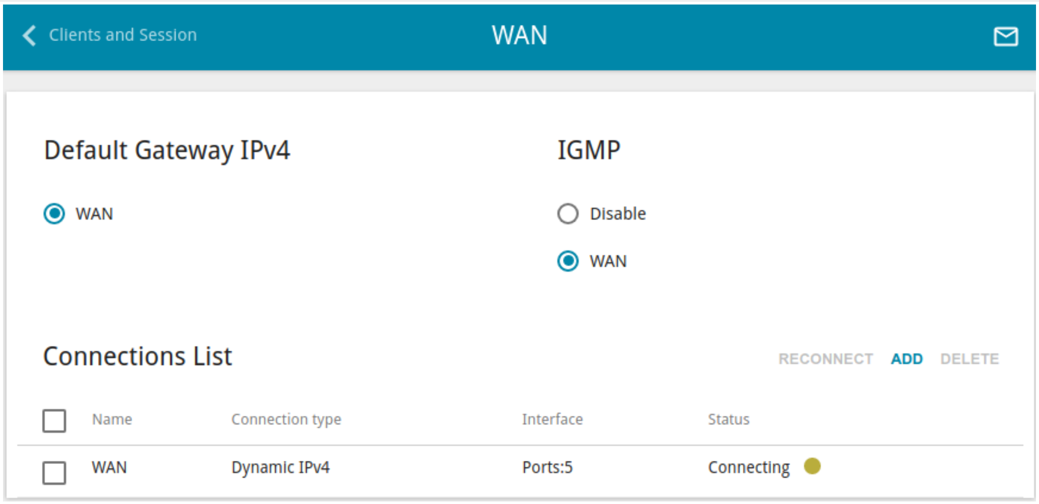
Connections Setup

In this menu you can configure basic parameters of the router's local area network and configure connection to the Internet (a WAN connection).

WAN

On the **Connections Setup / WAN** page, you can create and edit connections used by the router.

By default, a **Dynamic IPv4** connection is configured in the system. It is assigned to the WAN port of the router. You can edit this connection or delete it.



□	Name	Connection type	Interface	Status
□	WAN	Dynamic IPv4	Ports:5	Connecting ●

*Figure 58. The **Connections Setup / WAN** page.*

To create a new connection, click the **ADD** button in the **Connections List** section. On the opened page, specify relevant parameters.

To edit an existing connection, in the **Connections List** section, left-click the relevant line in the table. On the opened page, change the parameters and click the **APPLY** button.

To disconnect a connection and establish it again, select the checkbox located to the left of the relevant line in the table and click the **RECONNECT** button.

On the **Basic** tab, mandatory settings of a WAN connection are displayed. To view all available settings of the needed WAN connection, go to the **All Settings** tab.

To remove a connection, in the **Connections List** section, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button. Also you can remove a connection on the editing page.

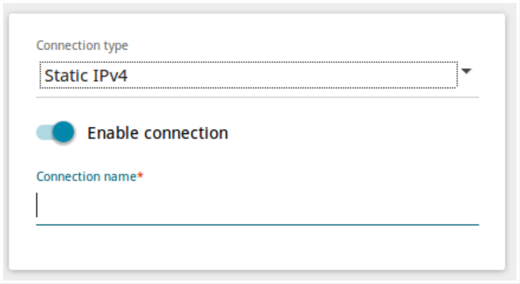
To allow multicast traffic (e.g. streaming video) for a connection, in the **IGMP** section, select the choice of the radio button which corresponds to this connection (only for connections of the Dynamic IPv4 or Static IPv4 type).

To forbid multicast traffic for all WAN connections, select the **Disable** choice of the radio button.

To use one of existing WAN connections as the default IPv4 or IPv6 connection, in the **Default Gateway** section, select the choice of the radio button which corresponds to this connection.

Creating Dynamic IPv4 or Static IPv4 WAN Connection

To create a connection of the Dynamic IPv4 or Static IPv4 type, click the **ADD** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection type** drop-down list and specify the needed values.



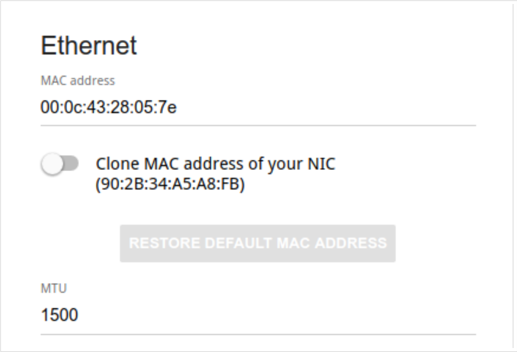
Connection type
Static IPv4

Enable connection

Connection name*

*Figure 59. The page for creating a new **Static IPv4** connection. Selecting a connection type.*

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.



Ethernet

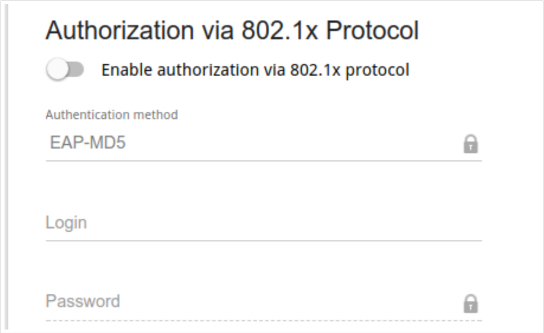
MAC address
00:0c:43:28:05:7e

Clone MAC address of your NIC (90:2B:34:A5:A8:FB)

MTU
1500

*Figure 60. The page for creating a new **Static IPv4** connection. The **Ethernet** section.*

Parameter	Description
Ethernet	
MAC address	A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement. To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, move the **Clone MAC address of your NIC** switch to the right. When the switch is moved to the right, the field is unavailable for editing. To set the router's MAC address, click the **RESTORE DEFAULT MAC ADDRESS** button (the button is available when the switch is moved to the right).
MTU	The maximum size of units transmitted by the interface.



Authorization via 802.1x Protocol

Enable authorization via 802.1x protocol

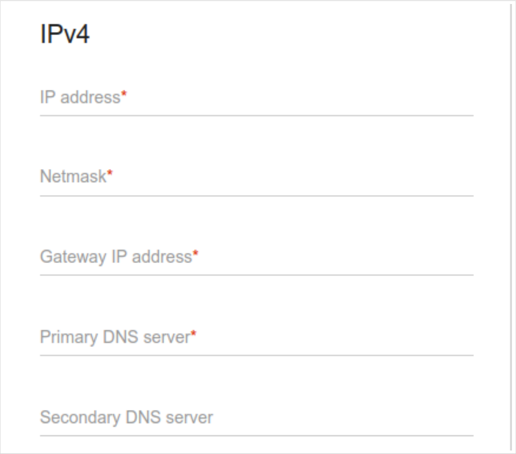
Authentication method: EAP-MD5

Login

Password

*Figure 61. The page for creating a new **Static IPv4** connection. The **Authorization via 802.1x Protocol** section.*

Parameter	Description
Authorization via 802.1x Protocol	
Enable authorization via 802.1x protocol	Move the switch to the right to allow authorization in the ISP's network via the 802.1x protocol.
Authentication method	Select a needed authentication method from the drop-down list.
Login	Enter the username provided by your ISP.
Password	Enter the password provided by your ISP.



IPv4

IP address*

Netmask*

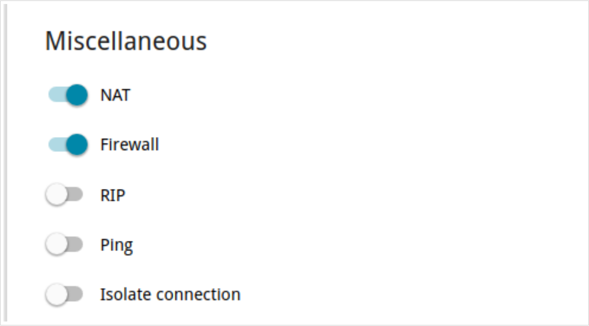
Gateway IP address*

Primary DNS server*

Secondary DNS server

Figure 62. The page for creating a new ***Static IPv4*** *connection. The* ***IPv4*** *section.*

Parameter	Description
IPv4	
For ***Static IPv4*** *type*	
IP address	Enter an IP address for this WAN connection.
Netmask	Enter a subnet mask for this WAN connection.
Gateway IP address	Enter an IP address of the gateway used by this WAN connection.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
For ***Dynamic IPv4*** *type*	
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of DNS server addresses. Upon that the **Primary DNS server** and **Secondary DNS server** fields are not available for editing.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
Vendor ID	The identifier of your ISP. *Optional*.
Hostname	A name of the router specified by your ISP. *Optional*.



Miscellaneous

● NAT

● Firewall

○ RIP

○ Ping

○ Isolate connection

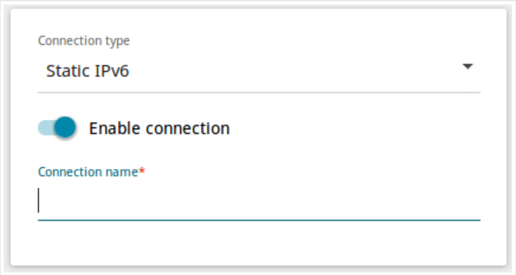
*Figure 63. The page for creating a new **Static IPv4** connection. The **Miscellaneous** section.*

Parameter	Description
Miscellaneous	
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
RIP	Move the switch to the right to allow using RIP for this connection.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

When all needed settings are configured, click the **APPLY** button.

Creating Dynamic IPv6 or Static IPv6 WAN Connection

To create a connection of the Dynamic IPv6 or Static IPv6 type, click the **ADD** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection type** drop-down list and specify the needed values.



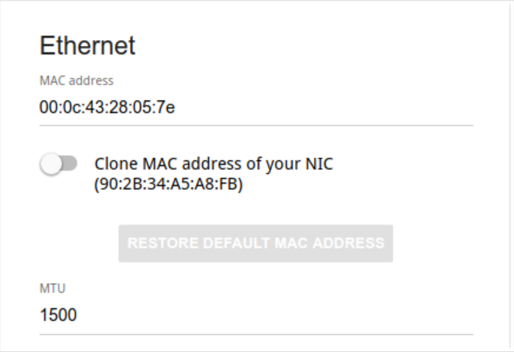
Connection type: Static IPv6

Enable connection: ON

Connection name*:

*Figure 64. The page for creating a new **Static IPv6** connection. Selecting a connection type.*

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.



Ethernet

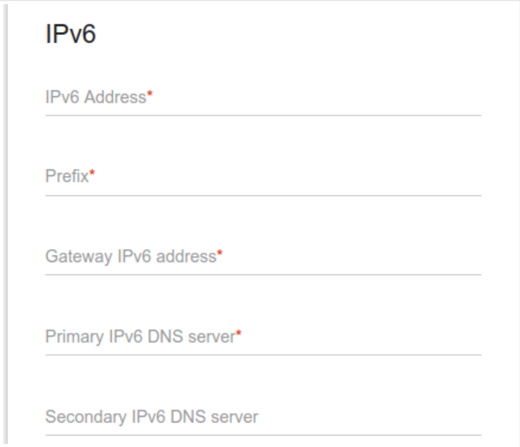
MAC address
00:0c:43:28:05:7e

○ Clone MAC address of your NIC (90:2B:34:A5:A8:FB)

MTU
1500

*Figure 65. The page for creating a new **Static IPv6** connection. The **Ethernet** section.*

Parameter	Description
Ethernet	
MAC address	A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement. To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, move the **Clone MAC address of your NIC** switch to the right. When the switch is moved to the right, the field is unavailable for editing. To set the router's MAC address, click the **RESTORE DEFAULT MAC ADDRESS** button (the button is available when the switch is moved to the right).
MTU	The maximum size of units transmitted by the interface.



IPv6

IPv6 Address*

Prefix*

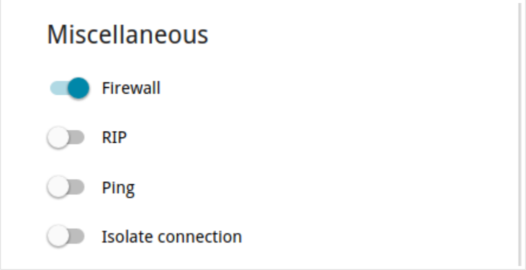
Gateway IPv6 address*

Primary IPv6 DNS server*

Secondary IPv6 DNS server

*Figure 66. The page for creating a new **Static IPv6** connection. The **IPv6** section.*

Parameter	Description
IPv6	
*For **Static IPv6** type*	
IPv6 Address	Enter an IPv6 address for this WAN connection.
Prefix	The length of the subnet prefix. The value 64 is used usually.
Gateway IPv6 address	Enter an IPv6 address of the gateway used by this WAN connection.
Primary IPv6 DNS server/Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.
*For **Dynamic IPv6** type*	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the **Automatically** value.
Gateway by SLAAC	Move the switch to the right to automatically assign the IPv6 gateway address with help of SLAAC (*Stateless Address Autoconfiguration*).
Gateway IPv6 address	The address of the IPv6 gateway. The field is available for editing, if the **Gateway by SLAAC** switch is moved to the left.
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the **Primary IPv6 DNS server** and **Secondary IPv6 DNS server** fields are not available for editing.
Primary IPv6 DNS server/Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.



Miscellaneous

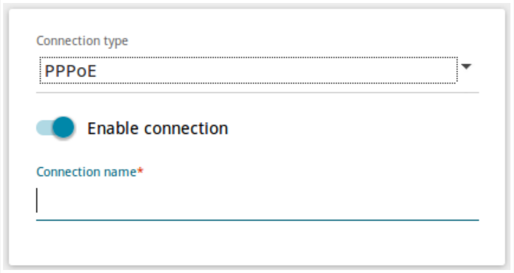
*Figure 67. The page for creating a new **Static IPv6** connection. The **Miscellaneous** section.*

Parameter	Description
Miscellaneous	
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
RIP	Move the switch to the right to allow using RIP for this connection.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

When all needed settings are configured, click the **APPLY** button.

Creating PPPoE WAN Connection

To create a connection of the PPPoE type, click the **ADD** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection type** drop-down list and specify the needed values.



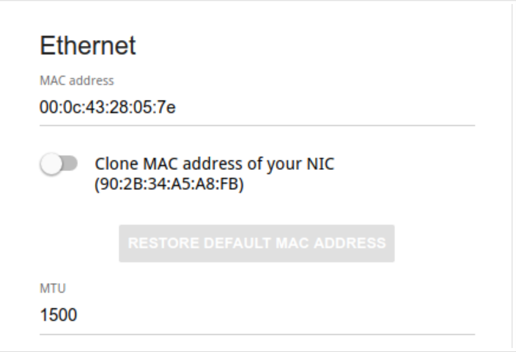
Connection type: PPPoE

Enable connection

Connection name*

*Figure 68. The page for creating a new **PPPoE** connection. Selecting a connection type.*

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.



Ethernet

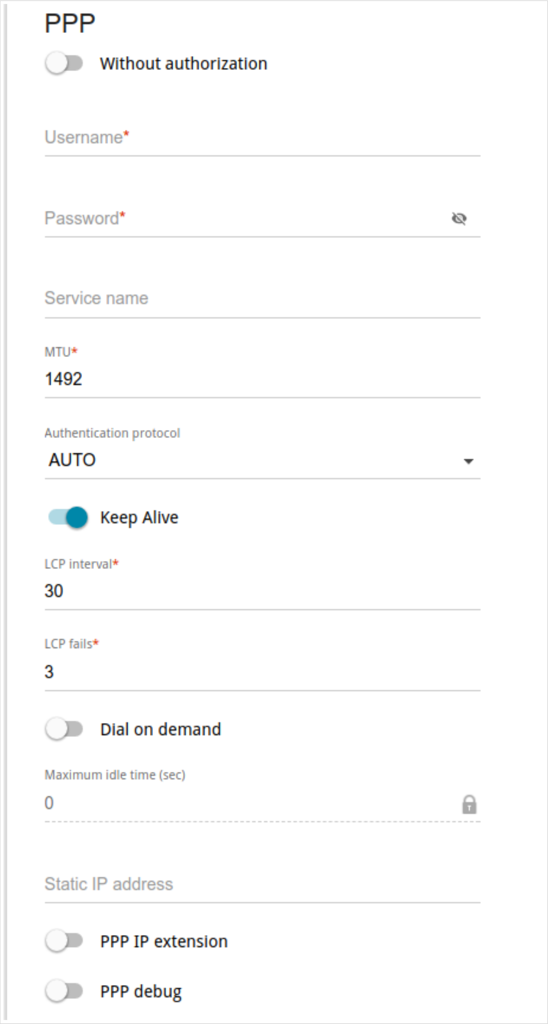
MAC address
00:0c:43:28:05:7e

○ Clone MAC address of your NIC (90:2B:34:A5:A8:FB)

MTU
1500

Figure 69. The page for creating a new ***PPPoE*** *connection. The* ***Ethernet*** *section.*

Parameter	Description
Ethernet	
MAC address	A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement. To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, move the **Clone MAC address of your NIC** switch to the right. When the switch is moved to the right, the field is unavailable for editing. To set the router's MAC address, click the **RESTORE DEFAULT MAC ADDRESS** button (the button is available when the switch is moved to the right).
MTU	The maximum size of units transmitted by the interface.



PPP

Without authorization

Username*

Password*

Service name

MTU*
1492

Authentication protocol
AUTO

Keep Alive

LCP interval*
30

LCP fails*
3

Dial on demand

Maximum idle time (sec)
0

Static IP address

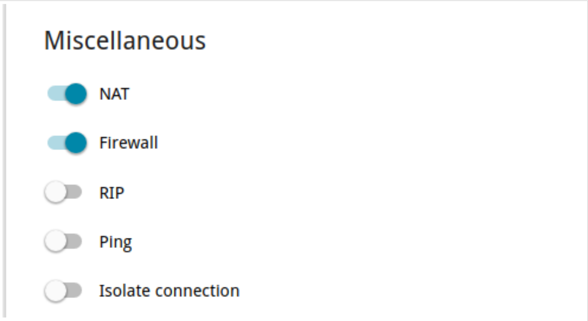
PPP IP extension

PPP debug

*Figure 70. The page for creating a new **PPPoE** connection. The **PPP** section.*

Parameter	Description
PPP	
Without authorization	Move the switch to the right if you don't need to enter a username and password to access the Internet.
Username	A username (login) to access the Internet.
Password	A password to access the Internet. Click the **Show** icon (👁) to display the entered password.
Service name	The name of the PPPoE authentication server.
MTU	The maximum size of units transmitted by the interface.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.

Parameter	Description
Keep Alive	Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the **LCP interval** and **LCP fails** fields are available. Specify the required values.
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the **Maximum idle time** field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Static IP address	Fill in the field if you want to use a static IP address to access the Internet.
PPP IP extension	This option is used by some ISPs. Contact your ISP to clarify if this option needs to be enabled. If it is required, move the switch to the right.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.



Miscellaneous

● NAT

● Firewall

○ RIP

○ Ping

○ Isolate connection

*Figure 71. The page for creating a new **PPPoE** connection. The **Miscellaneous** section.*

Parameter	Description
Miscellaneous	
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
RIP	Move the switch to the right to allow using RIP for this connection.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

When all needed settings are configured, click the **APPLY** button.

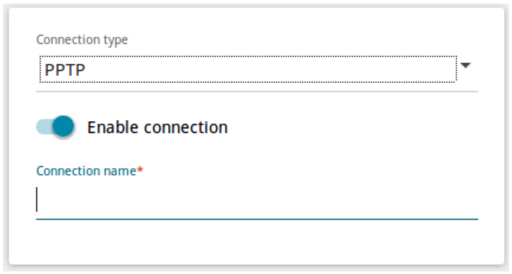
After clicking the button, the window for creating an additional connection opens.

If your ISP offers access to local services (e.g. audio and video resources), click the **CREATE** button. On the page displayed, specify the parameters for the connection of the Dynamic IPv4 or Static IPv4 type and click the **APPLY** button. Click the **BACK** button to specify other settings for the connection of the PPPoE type.

If you do not need to create an additional connection, click the **SKIP** button. In this case, the **Connections Setup / WAN** page opens.

Creating PPTP or L2TP WAN Connection

To create a connection of the PPTP or L2TP type, click the **ADD** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection type** drop-down list and specify the needed values.



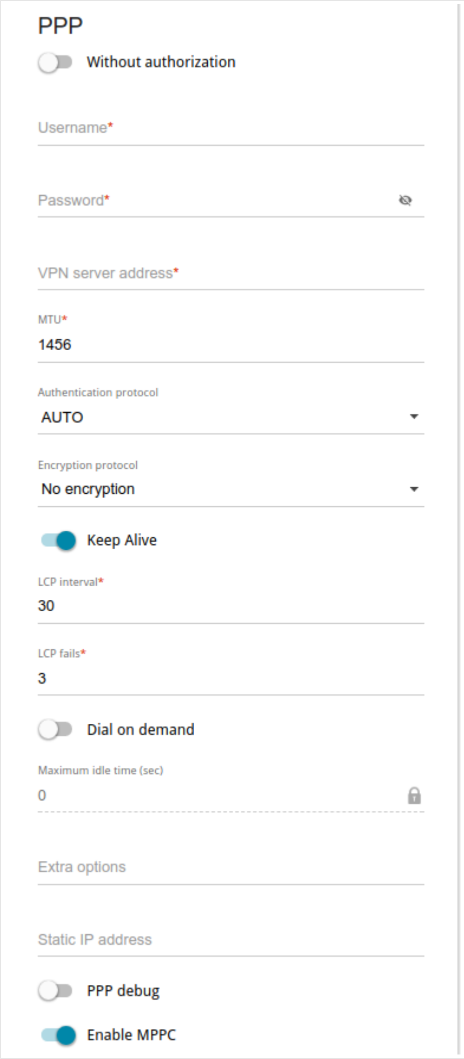
Connection type
PPTP

Enable connection

Connection name*

*Figure 72. The page for creating a new **PPTP** connection. Selecting a connection type.*

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.



PPP

○ Without authorization

Username*

Password*

VPN server address*

MTU*
1456

Authentication protocol
AUTO

Encryption protocol
No encryption

● Keep Alive

LCP interval*
30

LCP fails*
3

○ Dial on demand

Maximum idle time (sec)
0

Extra options

Static IP address

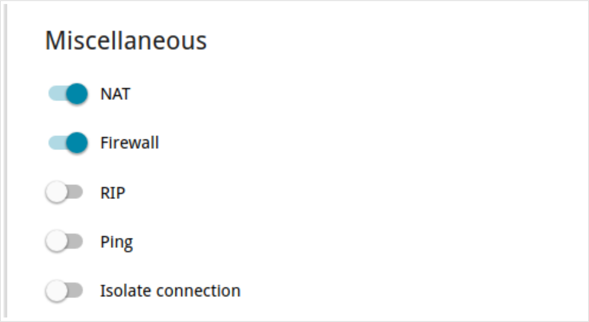
○ PPP debug

● Enable MPPC

*Figure 73. The page for creating a new **PPTP** connection. The **PPP** section.*

Parameter	Description
PPP	
Without authorization	Move the switch to the right if you don't need to enter a username and password to access the Internet.
Username	A username (login) to access the Internet.
Password	A password to access the Internet. Click the **Show** icon (👁) to display the entered password.
VPN server address	The IP or URL address of the PPTP or L2TP authentication server.
MTU	The maximum size of units transmitted by the interface.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.

Parameter	Description
Encryption protocol	Select a method of MPPE encryption. • **No encryption**: MPPE encryption is not applied. • **MPPE 40/128 bit**: MPPE encryption with a 40-bit or 128-bit key is applied. • **MPPE 40 bit**: MPPE encryption with a 40-bit key is applied. • **MPPE 128 bit**: MPPE encryption with a 128-bit key is applied. MPPE encryption can be applied only if the **MS-CHAP, MS-CHAPV2**, or **AUTO** value is selected from the **Authentication protocol** drop-down list.
Keep Alive	Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the **LCP interval** and **LCP fails** fields are available. Specify the required values.
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the **Maximum idle time** field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Extra options	Advanced options of the pppd daemon which need to be specified for this connection. *Optional*.
Static IP address	Fill in the field if you want to use a static IP address to access the Internet.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.
Enable MPPC	*(Microsoft Point-to-Point Compression)* *For the* ***PPTP*** *type only.* Move the switch to the right if it is necessary to use the data compression function in order to configure the connection. Move the switch to the left to disable the function.



Miscellaneous

● NAT

● Firewall

○ RIP

○ Ping

○ Isolate connection

*Figure 74. The page for creating a new **PPTP** connection. The **Miscellaneous** section.*

Parameter	Description
Miscellaneous	
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
RIP	Move the switch to the right to allow using RIP for this connection.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

When all needed settings are configured, click the **APPLY** button.

After clicking the button, the window for additional configuration of the connection opens.

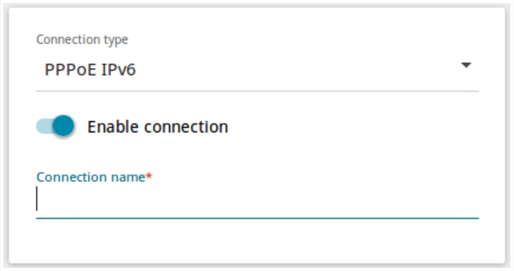
If you want to use this WAN connection to access the Internet, select the **to the Internet** choice of the radio button. Then select the existing connection which will be used to access the PPTP/L2TP server or select the **create a new connection** choice of the radio button.

If you have already configured the connection to the Internet and you want to use this WAN connection only to connect to the virtual private network, select the **to the virtual private network** choice of the radio button.

Click the **OK** button.

Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection

To create a connection of the PPPoE IPv6 or PPPoE Dual Stack type, click the **ADD** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection type** drop-down list and specify the needed values.



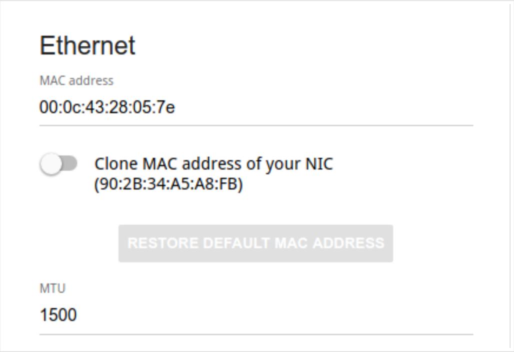
Connection type
PPPoE IPv6

Enable connection

Connection name*

*Figure 75. The page for creating a new **PPPoE IPv6** connection. Selecting a connection type.*

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.


Ethernet

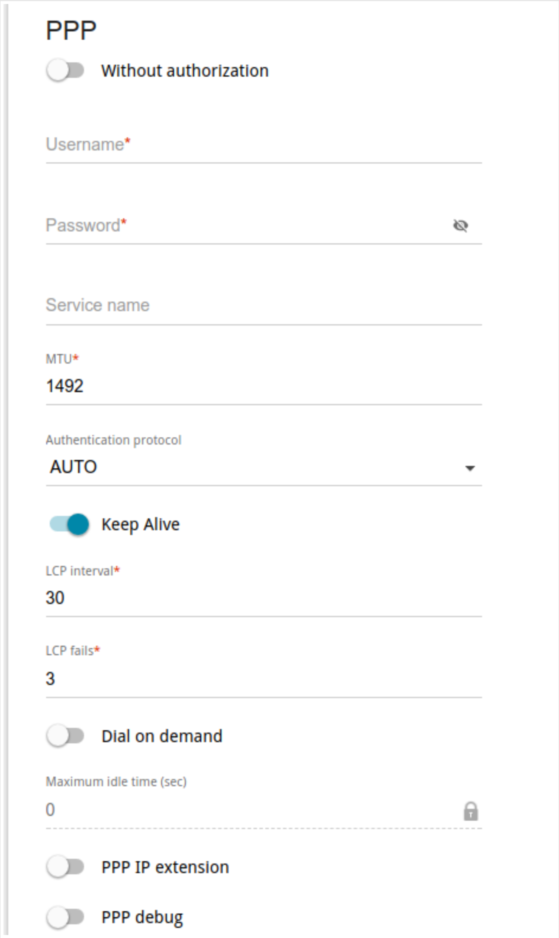
MAC address
00:0c:43:28:05:7e

Clone MAC address of your NIC (90:2B:34:A5:A8:FB)

MTU
1500

Figure 76. The page for creating a new ***PPPoE IPv6*** *connection. The* ***Ethernet*** *section.*

Parameter	Description
Ethernet	
MAC address	A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement. To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, move the **Clone MAC address of your NIC** switch to the right. When the switch is moved to the right, the field is unavailable for editing. To set the router's MAC address, click the **RESTORE DEFAULT MAC ADDRESS** button (the button is available when the switch is moved to the right).
MTU	The maximum size of units transmitted by the interface.



PPP

○ Without authorization

Username*

Password*

Service name

MTU*
1492

Authentication protocol
AUTO

● Keep Alive

LCP interval*
30

LCP fails*
3

○ Dial on demand

Maximum idle time (sec)
0

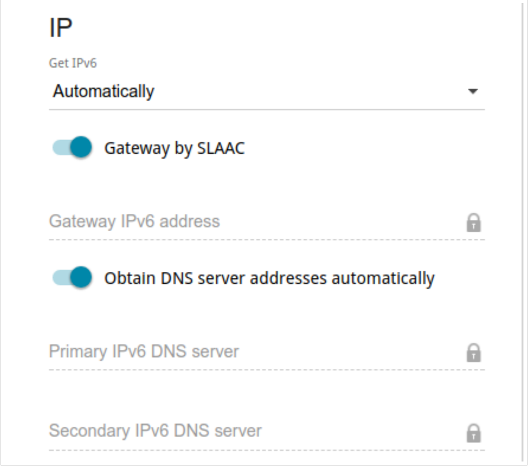
○ PPP IP extension

○ PPP debug

*Figure 77. The page for creating a new **PPPoE IPv6** connection. The **PPP** section.*

Parameter	Description
PPP	
Without authorization	Move the switch to the right if you don't need to enter a username and password to access the Internet.
Username	A username (login) to access the Internet.
Password	A password to access the Internet. Click the **Show** icon (👁) to display the entered password.
Service name	The name of the PPPoE authentication server.
MTU	The maximum size of units transmitted by the interface.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.

Parameter	Description
Keep Alive	Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the **LCP interval** and **LCP fails** fields are available. Specify the required values.
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the **Maximum idle time** field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Static IP address	*For the* ***PPPoE Dual Stack*** *type only.* Fill in the field if you want to use a static IP address to access the Internet.
PPP IP extension	This option is used by some ISPs. Contact your ISP to clarify if this option needs to be enabled. If it is required, move the switch to the right.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.



IP

Get IPv6: Automatically

● Gateway by SLAAC

Gateway IPv6 address

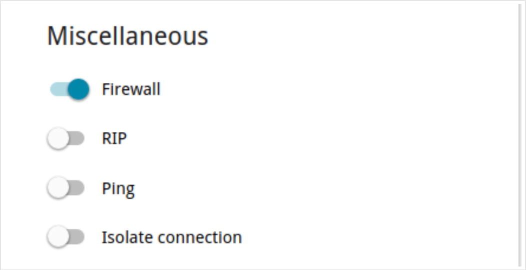
● Obtain DNS server addresses automatically

Primary IPv6 DNS server

Secondary IPv6 DNS server

*Figure 78. The page for creating a new **PPPoE Pv6** connection. The **IP** section.*

Parameter	Description
IP	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the **Automatically** value.
Gateway by SLAAC	Move the switch to the right to automatically assign the IPv6 gateway address with help of SLAAC (*Stateless Address Autoconfiguration*).
Gateway IPv6 address	The address of the IPv6 gateway. The field is available for editing, if the **Gateway by SLAAC** switch is moved to the left.
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the **Primary IPv6 DNS server** and **Secondary IPv6 DNS server** fields are not available for editing.
Primary IPv6 DNS server/Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.



Miscellaneous

● Firewall

○ RIP

○ Ping

○ Isolate connection

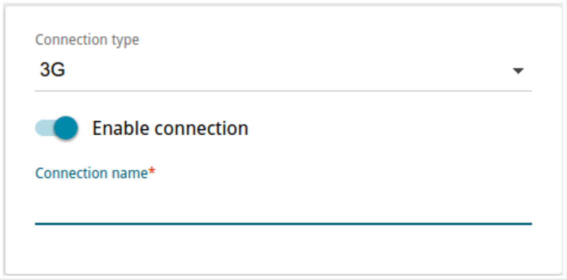
*Figure 79. The page for creating a new **PPPoE IPv6** connection. The **Miscellaneous** section.*

Parameter	Description
Miscellaneous	
NAT	*For the* ***PPPoE Dual Stack*** *type only.* If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
RIP	Move the switch to the right to allow using RIP for this connection.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

When all needed settings are configured, click the **APPLY** button.

Creating 3G WAN Connection

If the PIN code check is enabled for the SIM card inserted into your USB modem, then prior to creating a 3G WAN connection, go to the **USB Modem** menu and enter the PIN code on the page displayed (see the ***USB Modem*** section, page 152). Then go to the **Connections Setup / WAN** page and click the **ADD** button in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection type** drop-down list and specify the needed values.



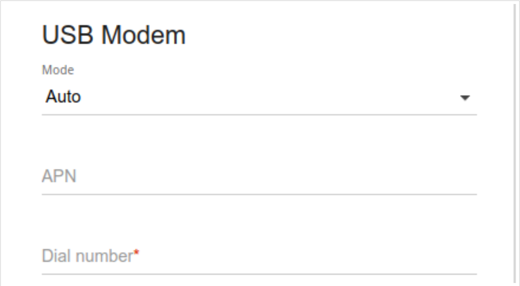
Connection type
3G

Enable connection

Connection name*

*Figure 80. The page for creating a new **3G** connection. Selecting a connection type.*

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.



USB Modem

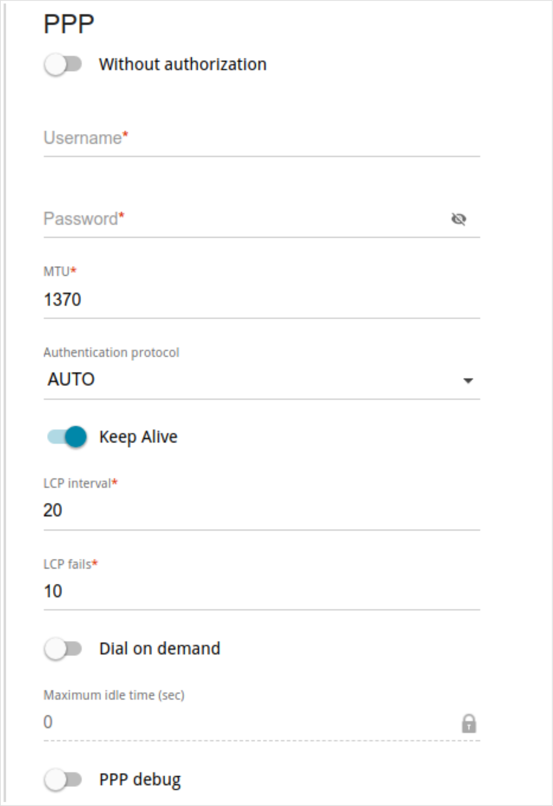
Mode
Auto

APN

Dial number*

*Figure 81. The page for creating a new **3G** connection. The **USB Modem** section.*

Parameter	Description
USB Modem	
Mode	The value of the field specifies the type of the network to which the router connects. Leave the **Auto** value to let the router connect automatically to an available type of network, or select a needed value from the drop-down list.
APN	An access point name.
Dial number	A number dialed to connect to the authorization server of the operator.



PPP

○ Without authorization

Username*

Password*

MTU*
1370

Authentication protocol
AUTO

● Keep Alive

LCP interval*
20

LCP fails*
10

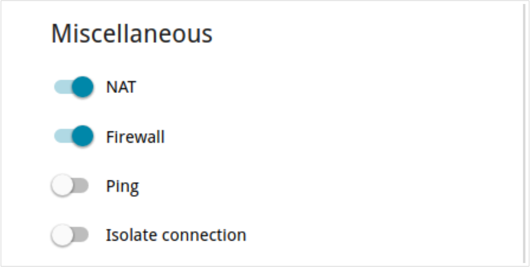
○ Dial on demand

Maximum idle time (sec)
0

○ PPP debug

*Figure 82. The page for creating a new **3G** connection. The **PPP** section.*

Parameter	Description
PPP	
Without authorization	Move the switch to the right if your operator does not require authorization.
Username	A username (login) to connect to the network of the operator.
Password	A password to connect to the network of the operator. Click the **Show** icon (👁) to display the entered password.
MTU	The maximum size of units transmitted by the interface.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.
Keep Alive	Move the switch to the right if you want the router to keep you connected to the network of your operator even when the connection has been inactive for a specified period of time. When the checkbox is selected, the **LCP interval** and **LCP fails** fields are available. Specify the required values.
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the **Maximum idle time** field, specify a period of inactivity (in seconds) after which the connection should be terminated.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.



Miscellaneous

● NAT

● Firewall

○ Ping

○ Isolate connection

*Figure 83. The page for creating a new **3G** connection. The **Miscellaneous** section.*

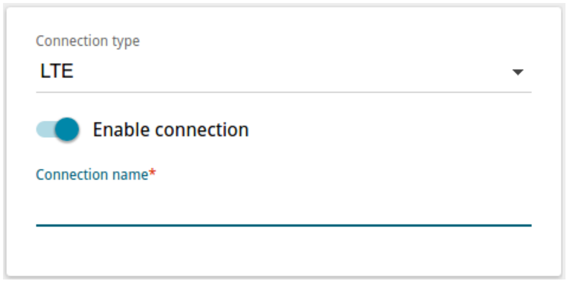
Parameter	Description
Miscellaneous	
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

When all needed settings are configured, click the **APPLY** button.

Creating LTE WAN Connection

! For the USB modem Megafon M100-1, please reboot the router after creating the WAN connection.

If the PIN code check is enabled for the SIM card inserted into your USB modem, then prior to creating an LTE WAN connection, go to the **USB Modem** menu and enter the PIN code[10] on the page displayed (see the ***USB Modem*** section, page 152). Then go to the **Connections Setup / WAN** page and click the **ADD** button in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection type** drop-down list and specify the needed values.



Connection type: LTE

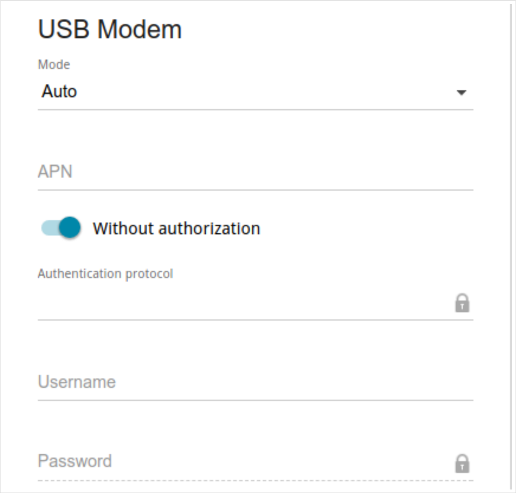
Enable connection

Connection name*

*Figure 84. The page for creating a new **LTE** connection. Selecting a connection type.*

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.

[10] For some models of LTE USB modems it is required to disable the PIN code check on the SIM card prior to connecting the USB modem to the router.



USB Modem

Mode
Auto

APN

Without authorization

Authentication protocol

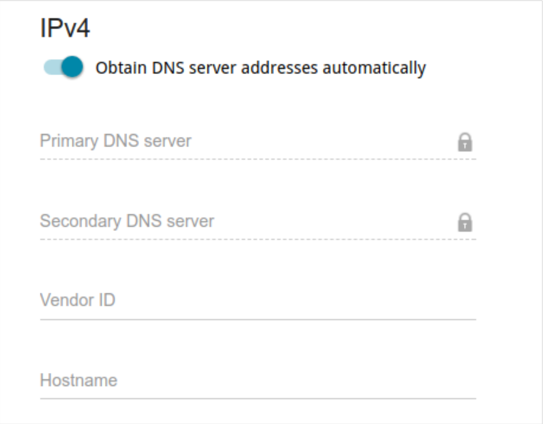
Username

Password

*Figure 85. The page for creating a new **LTE** connection. The **USB Modem** section.*

Parameter	Description
USB Modem	
Mode	The value of the field specifies the type of the network to which the router connects. Leave the **Auto** value to let the router connect automatically to an available type of network, or select a needed value from the drop-down list.[11]
APN	An access point name.
Without authorization	Move the switch to the right if your operator does not require authorization.
Authentication protocol	Select a required authentication method from the drop-down list.
Username	A username (login) to connect to the network of the operator.
Password	A password to connect to the network of the operator. Click the **Show** icon (👁) to display the entered password.

[11] Some LTE USB modems do not support network type selection and work in the **Auto** mode regardless of the value selected from the drop-down list.



IPv4

Obtain DNS server addresses automatically

Primary DNS server

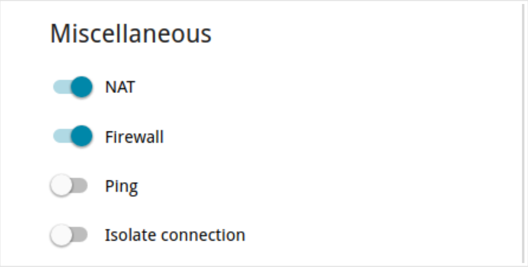
Secondary DNS server

Vendor ID

Hostname

*Figure 86. The page for creating a new **LTE** connection. The **IPv4** section.*

Parameter	Description
IPv4	
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of DNS server addresses. Upon that the **Primary DNS server** and **Secondary DNS server** fields are not available for editing.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
Vendor ID	The identifier of your ISP. *Optional*.
Hostname	A name of the router specified by your ISP. *Optional*.



Miscellaneous

● NAT

● Firewall

○ Ping

○ Isolate connection

*Figure 87. The page for creating a new **LTE** connection. The **Miscellaneous** section.*

Parameter	Description
Miscellaneous	
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

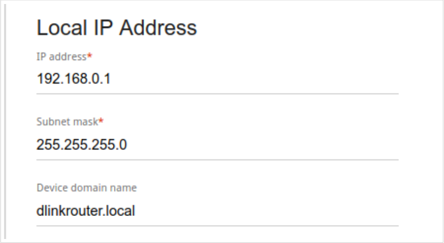
When all needed settings are configured, click the **APPLY** button.

LAN

To configure the router's local interface, go to the **Connections Setup / LAN** page.

IPv4

Go to the **IPv4** tab to change IPv4 address, configure the built-in DHCP server, or specify MAC address and IP address pairs.



Local IP Address

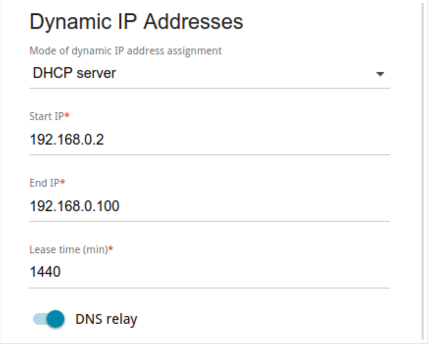
IP address*
192.168.0.1

Subnet mask*
255.255.255.0

Device domain name
dlinkrouter.local

*Figure 88. Configuring the local interface. The **IPv4** tab. The **Local IP Address** section.*

Parameter	Description
Local IP Address	
Mode of local IP address assignment	*For the **Access point**, **Repeater**, and **Client modes** only.* Select the needed value from the drop-down list. **Static**: the IP address, subnet mask, and the gateway IP address are assigned manually. **Dynamic**: the router automatically obtains these parameters from the LAN DHCP server or from the router to which it connects.
IP address	The IP address of the router in the local subnet. By default, the following value is specified: `192.168.0.1`.
Subnet mask	The mask of the local subnet. By default, the following value is specified: `255.255.255.0`.
Gateway IP address	*For the **Access point**, **Repeater**, and **Client** modes only.* The gateway IP address which is used by the router to connect to the Internet (e.g., for synchronizing the system time with an NTP server). *Optional*.
Device domain name	The name of the device attached to its IP address in the local subnet.



Dynamic IP Addresses

Mode of dynamic IP address assignment: DHCP server

Start IP*: 192.168.0.2

End IP*: 192.168.0.100

Lease time (min)*: 1440

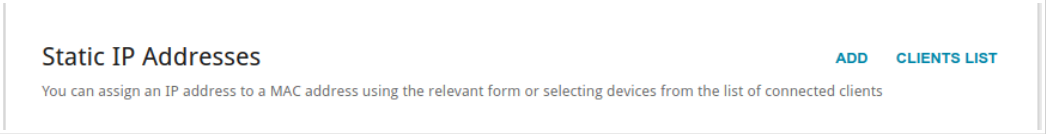
DNS relay

*Figure 89. Configuring the local interface. The **IPv4** tab. The **Dynamic IP Addresses** section.*

Parameter	Description
Dynamic IP Addresses	
Mode of dynamic IP address assignment	An operating mode of the router's DHCP server. **Disable**: the router's DHCP server is disabled, clients' IP addresses are assigned manually. **DHCP server**: the router assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the **Start IP**, **End IP**, **Lease time** fields and the **DNS relay** switch are displayed on the tab. **DHCP relay**: an external DHCP server is used to assign IP addresses to clients. When this value is selected, the **External DHCP server IP** field is displayed on the tab.
Start IP	The start IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
End IP	The end IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
Lease time	The lifetime of IP addresses leased by the DHCP server. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address.
DNS relay	Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address. Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the **Advanced / DNS** page as the DNS server address.
External DHCP server IP	The IP address of the external DHCP server which assigns IP addresses to the router's clients.

When all needed settings are configured, click the **APPLY** button.

In the **Static IP Addresses** section, you can specify MAC address and IP address pairs (set a fixed IPv4 address in the local area network for a device with a certain MAC address). The router assigns IP addresses in accordance with the specified pairs only when the DHCP server is enabled (in the **Dynamic IP Addresses** section, the **DHCP server** value is selected from the **Mode of dynamic IP address assignment** drop-down list).



Static IP Addresses

You can assign an IP address to a MAC address using the relevant form or selecting devices from the list of connected clients

Figure 90. The section for creating MAC-IP pairs.

To create a MAC-IP pair, click the **ADD** button. In the opened window, in the **MAC address** field, enter the MAC address of the device from the LAN, then in the **IP address** field, enter an IPv4 address which will be assigned to it. In the **Host** field, specify a network name of the device for easier identification (*optional*). Click the **APPLY** button.

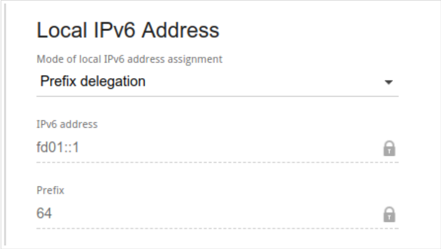
In order to view MAC addresses of the devices connected to the router at the moment, click the **CLIENTS LIST** button. In the opened window, select the needed device and click the **OK** button. To view the latest list of the connected devices, click the **REFRESH** button.

To edit an existing MAC-IP pair, left-click the relevant line in the table. In the opened window, change the needed parameters and click the **APPLY** button.

To remove a MAC-IP pair, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button. Then click the **APPLY** button. Also you can remove a MAC-IP pair in the editing window.

IPv6

Go to the **IPv6** tab to change IPv6 address of the router and configure IPv6 addresses assignment settings.



Local IPv6 Address

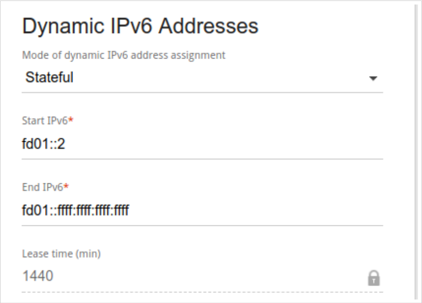
Mode of local IPv6 address assignment: Prefix delegation

IPv6 address: fd01::1

Prefix: 64

*Figure 91. Configuring the local interface. The **IPv6** tab. The **Local IPv6 Address** section.*

Parameter	Description
Local IPv6 Address	
Mode of local IPv6 address assignment	Select the needed value from the drop-down list. **Static**: an IPv6 address and a prefix are specified manually. **Prefix delegation**: the router requests a prefix to configure an IPv6 address from a delegating router.
IPv6 address	The IPv6 address of the router in the local subnet. By default, the following value is specified: `fd01::1`. The field is available for editing, if the **Static** value is selected from the **Mode of local IPv6 address assignment** drop-down list.
Prefix	The length of the prefix subnet. By default, the value `64` is specified. The field is available for editing, if the **Static** value is selected from the **Mode of local IPv6 address assignment** drop-down list.



Dynamic IPv6 Addresses

Mode of dynamic IPv6 address assignment: Stateful

Start IPv6*: fd01::2

End IPv6*: fd01::ffff:ffff:ffff:ffff

Lease time (min): 1440

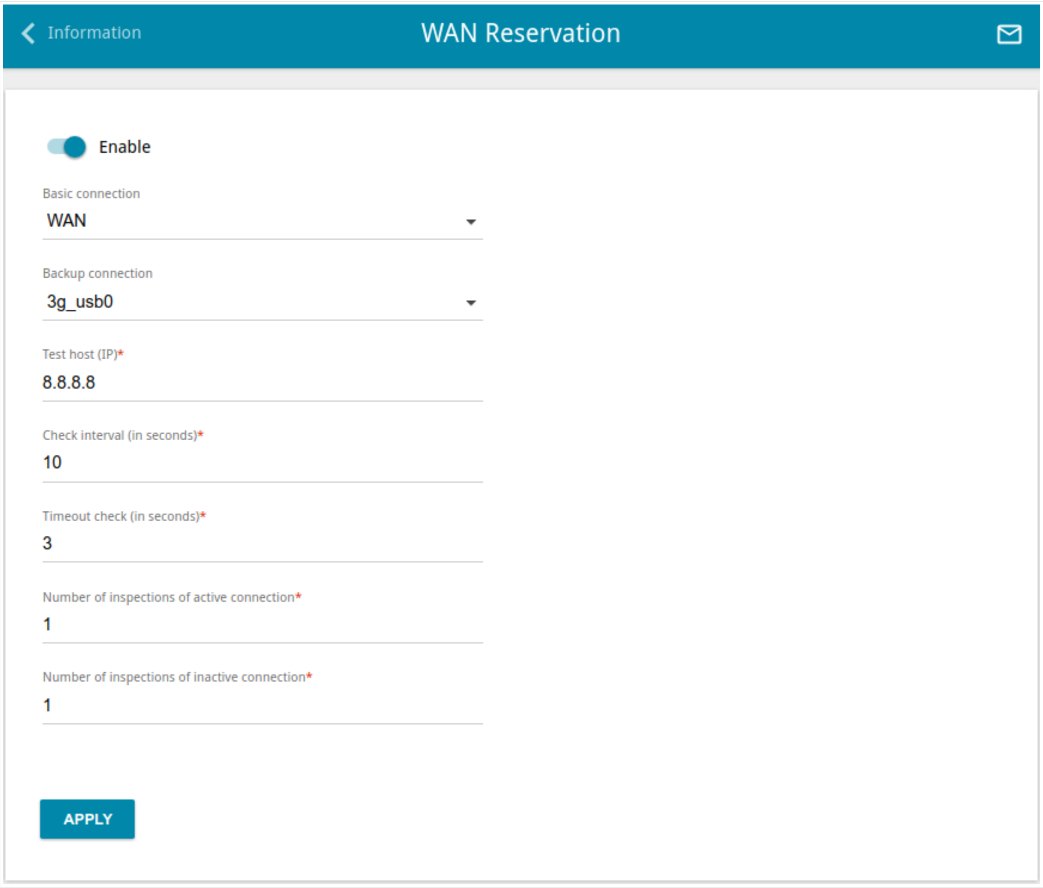
*Figure 92. Configuring the local interface. The **IPv6** tab. The **Dynamic IPv6 Addresses** section.*

Parameter	Description
Dynamic IPv6 Addresses	
Mode of dynamic IPv6 address assignment	Select the needed value from the drop-down list. **Disable**: clients' IPv6 addresses are assigned manually. **Stateful**: the built-in DHCPv6 server of the router allocates addresses from the range specified in the **Start IPv6** and **End IPv6** fields. **Stateless**: clients themselves configure IPv6 addresses using the prefix.
Start IPv6	The start IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
End IPv6	The end IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
Lease Time	The lifetime of IPv6 addresses provided to clients. The field is available for editing, if the **Static** value is selected from the **Mode of local IPv6 address assignment** list in the **Local IPv6 Address** section.

When all needed settings are configured, click the **APPLY** button.

WAN Reservation

On the **Connections Setup / WAN Reservation** page, you can enable the WAN backup function, which provides you with uninterrupted access to the Internet. When your main connection breaks down, the router activates the backup connection; and when the main channel is recovered, the router switches to it and disconnects the reserve one.



Enable

Basic connection
WAN

Backup connection
3g_usb0

Test host (IP)*
8.8.8.8

Check interval (in seconds)*
10

Timeout check (in seconds)*
3

Number of inspections of active connection*
1

Number of inspections of inactive connection*
1

*Figure 93. The **Connections Setup / WAN Reservation** page.*

To activate the backup function, create the main and the reserve WAN connections. After that go to the **Connections Setup / WAN Reservation** page, move the **Enable** switch to the right, and specify the needed values in the fields displayed on the page.

Parameter	Description
Basic connection	From the drop-down list, select a WAN connection which will be used as the main one.
Backup connection	From the drop-down list, select a WAN connection which will be used as the reserve one.
Test host	An IP address that the router will check for availability via ICMP ping mechanism.
Check interval	A time period (in seconds) between attempts to check the status of the main connection. By default, the value `10` is specified.

Parameter	Description
Timeout check	A time period (in seconds) for an attempt to check the status of the main connection. At the end of this period the router's internal system makes a decision to enable/disable the reserve channel. By default, the value **3** is specified.
Number of inspections of active connection	A number of requests that will be sent in order to analyze the status of the main connection when the connection is active (the router uses the main connection as a default gateway).
Number of inspections of inactive connection	A number of requests that will be sent in order to analyze the status of the main connection when the connection is inactive (the router uses the reserve connection as a default gateway).

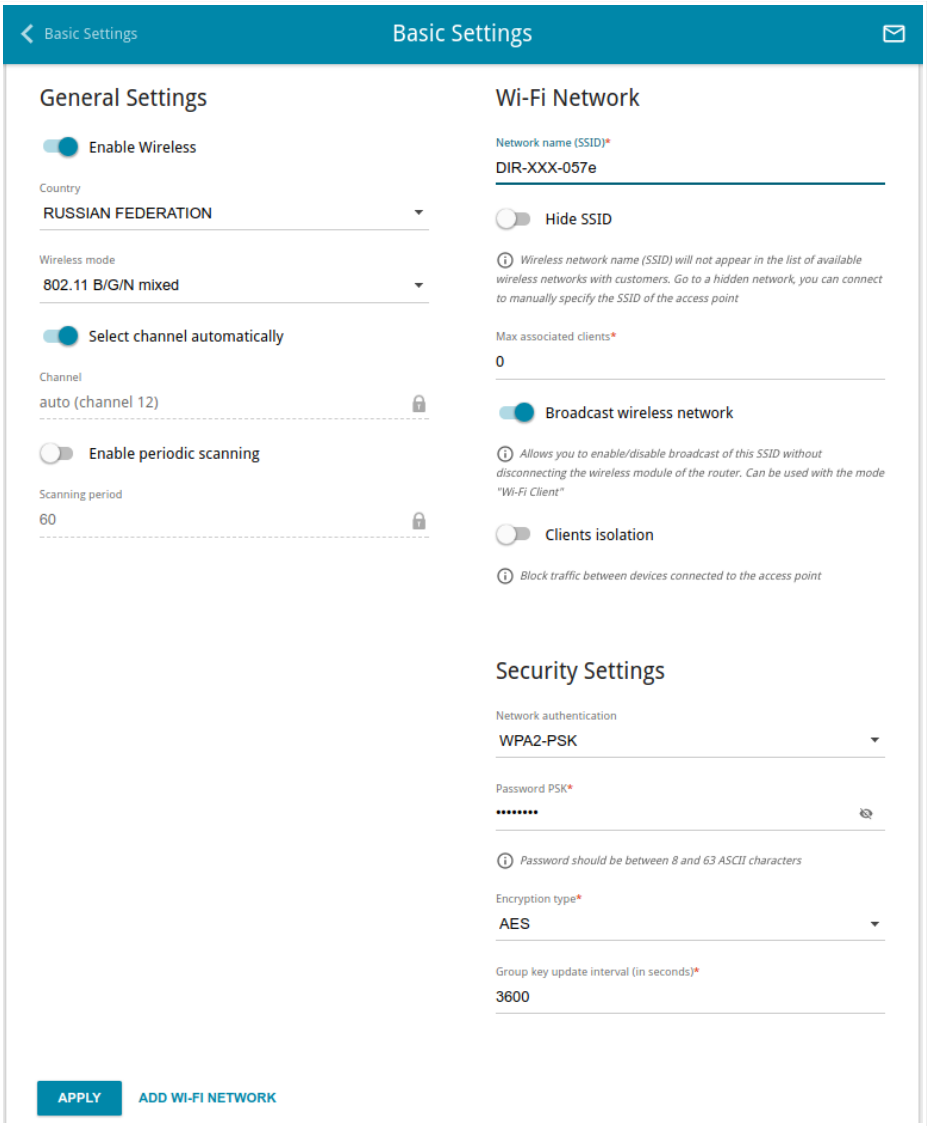
When all needed settings are configured, click the **APPLY** button.

Wi-Fi

In this menu you can specify all needed settings for your wireless network.

Basic Settings

In the **Wi-Fi / Basic Settings** section, you can change basic parameters for the wireless interface of the router and configure the basic and additional wireless networks. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.



General Settings

Enable Wireless

Country: RUSSIAN FEDERATION

Wireless mode: 802.11 B/G/N mixed

Select channel automatically

Channel: auto (channel 12)

Enable periodic scanning

Scanning period: 60

Wi-Fi Network

Network name (SSID)*: DIR-XXX-057e

Hide SSID

Wireless network name (SSID) will not appear in the list of available wireless networks with customers. Go to a hidden network, you can connect to manually specify the SSID of the access point

Max associated clients*: 0

Broadcast wireless network

Allows you to enable/disable broadcast of this SSID without disconnecting the wireless module of the router. Can be used with the mode "Wi-Fi Client"

Clients isolation

Block traffic between devices connected to the access point

Security Settings

Network authentication: WPA2-PSK

Password PSK*: ••••••••

Password should be between 8 and 63 ASCII characters

Encryption type*: AES

Group key update interval (in seconds)*: 3600

Figure 94. Basic settings of the wireless LAN in the 2.4GHz band.

In the **General Settings** section, the following parameters are available:

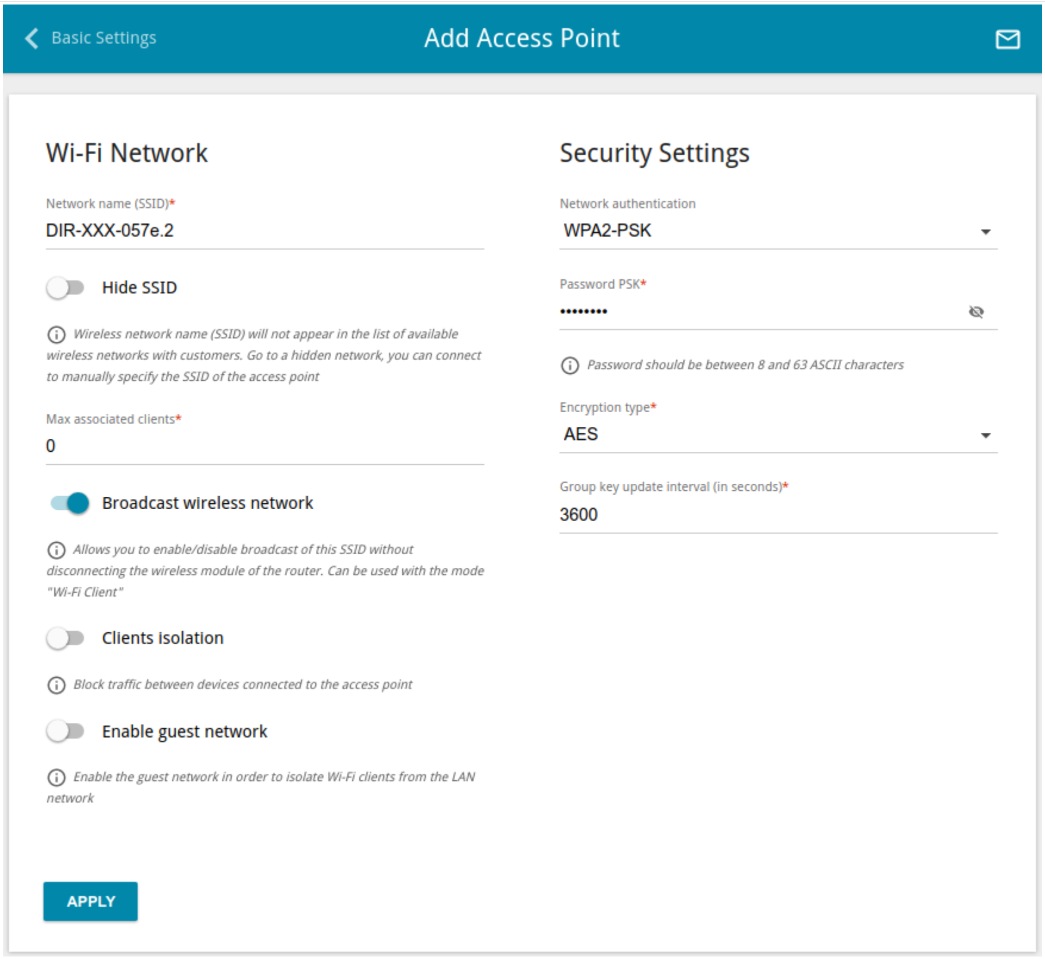
Parameter	Description
Enable Wireless	To enable Wi-Fi connection, move the switch to the right. To disable Wi-Fi connection, move the switch to the left.
Country	The country you are in. Select a value from the drop-down list.

Parameter	Description
Wireless mode	Operating mode of the wireless network of the router. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.
Select channel automatically	Move the switch to the right to let the router itself choose the channel with the least interference.
Channel	The wireless channel number. Left-click to open the window for selecting a channel (the action is available, when the **Select channel automatically** switch is moved to the left).
Enable periodic scanning	Move the switch to the right to let the router search for a free channel in certain periods of time. When the switch is moved to the right, the **Scanning period** field is available for editing.
Scanning period	Specify a period of time (in seconds) after which the router rescans channels.

When you have configured the parameters, click the **APPLY** button.

To edit the settings of the basic wireless network, in the **Wi-Fi Network** section, change the needed parameters and click the **APPLY** button.

Also you can create an additional wireless network. To do this, click the **ADD WI-FI NETWORK** button. On the opened page, specify the relevant parameters.



Wi-Fi Network

Network name (SSID)*: DIR-XXX-057e.2

Hide SSID

Wireless network name (SSID) will not appear in the list of available wireless networks with customers. Go to a hidden network, you can connect to manually specify the SSID of the access point

Max associated clients*: 0

Broadcast wireless network

Allows you to enable/disable broadcast of this SSID without disconnecting the wireless module of the router. Can be used with the mode "Wi-Fi Client"

Clients isolation

Block traffic between devices connected to the access point

Enable guest network

Enable the guest network in order to isolate Wi-Fi clients from the LAN network

Security Settings

Network authentication: WPA2-PSK

Password PSK*: ••••••••

Password should be between 8 and 63 ASCII characters

Encryption type*: AES

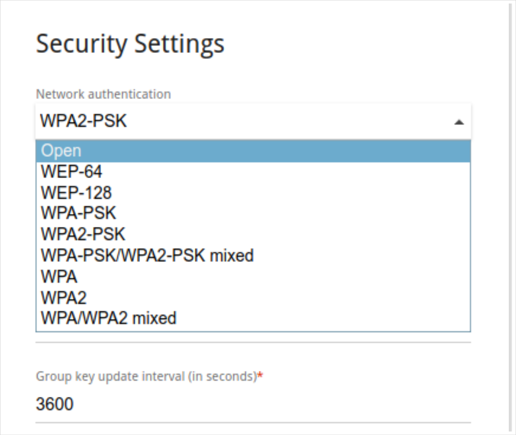
Group key update interval (in seconds)*: 3600

Figure 95. Creating a wireless network.

Parameter	Description
Wi-Fi Network	
Network name (SSID)	A name for the wireless network. The name can consist of digits and Latin characters.
Hide SSID	If the switch is moved to the right, other users cannot see your Wi-Fi network. It is recommended not to hide the network in order to simplify initial configuration of the wireless network.
BSSID	The unique identifier for this wireless network. You cannot change the value of this parameter, it is determined in the device's internal settings. The field is displayed in the settings of the existing wireless network.
Max Associated Clients	The maximum number of devices connected to the wireless network. When the value `0` is specified, the device does not limit the number of connected clients.
Broadcast wireless network	If the switch is moved to the left, devices cannot connect to the wireless network. Upon that the router can connect to another access point as a wireless client.
Clients isolation	Move the switch to the right to forbid wireless clients of this wireless network to communicate to each other.
Enable guest network	This function is available for the additional network. Move the switch to the right if you want the devices connected to the additional network to be isolated from the devices and resources of the router's LAN.

In the **Security Settings** section, you can change security settings of the wireless network.

By default, the **WPA2-PSK** network authentication type of both bands of the wireless network is specified. WPS PIN from the barcode label is used as the network key.



Security Settings

Network authentication

WPA2-PSK

- Open
- WEP-64
- WEP-128
- WPA-PSK
- WPA2-PSK
- WPA-PSK/WPA2-PSK mixed
- WPA
- WPA2
- WPA/WPA2 mixed

Group key update interval (in seconds)*

3600

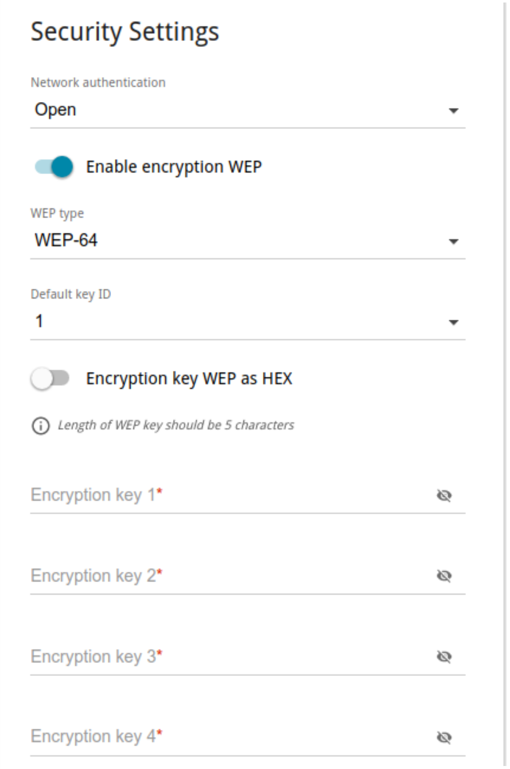
Figure 96. Network authentication types supported by the router.

The router supports the following authentication types:

Authentication type	Description
Open	Open authentication (with WEP encryption for wireless network modes not supporting 802.11n or 802.11ac devices).
WEP-64	Authentication with a 64-bit shared key with WEP encryption. This authentication type is not available when a mode supporting 802.11n or 802.11ac devices is selected from the **Wireless mode** drop-down list on the **Wi-Fi / Basic Settings** page.
WEP-128	Authentication with a 128-bit shared key with WEP encryption. This authentication type is not available when a mode supporting 802.11n or 802.11ac devices is selected from the **Wireless mode** drop-down list on the **Wi-Fi / Basic Settings** page.
WPA	WPA-based authentication using a RADIUS server.
WPA-PSK	WPA-based authentication using a PSK.
WPA2	WPA2-based authentication using a RADIUS server.
WPA2-PSK	WPA2-based authentication using a PSK.
WPA/WPA2 mixed	A mixed type of authentication. When this value is selected, devices using the **WPA** authentication type and devices using the **WPA2** authentication type can connect to the wireless network.
WPA-PSK/WPA2-PSK mixed	A mixed type of authentication. When this value is selected, devices using the **WPA-PSK** authentication type and devices using the **WPA2-PSK** authentication type can connect to the wireless network.

! The **WPA**, **WPA2**, and **WPA/WPA2 mixed** authentication types require a RADIUS server.

When the **Open**, **WEP-64**, or **WEP-128** value is selected, the following settings are displayed on the page (unavailable for the wireless network operating modes which support the standard 802.11n or 802.11ac):



Security Settings

Network authentication
Open

Enable encryption WEP

WEP type
WEP-64

Default key ID
1

Encryption key WEP as HEX

Length of WEP key should be 5 characters

Encryption key 1*

Encryption key 2*

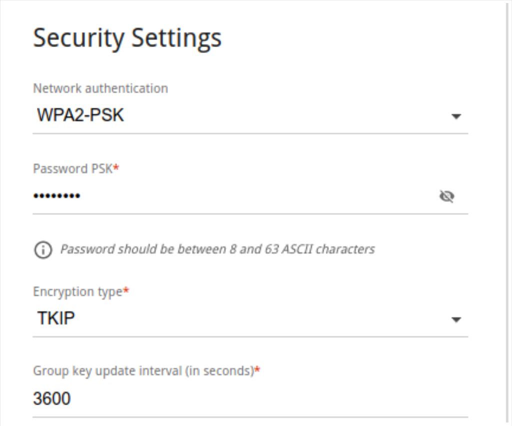
Encryption key 3*

Encryption key 4*

*Figure 97. The **Open** value is selected from the **Network authentication** drop-down list.*

Parameter	Description
Enable encryption WEP	*For **Open** authentication type only.* To activate WEP encryption, move the switch to the right. Upon that the **WEP type** and **Default key ID** drop-down lists, the **Encryption key WEP as HEX** switch, and four **Encryption key** fields are displayed on the page.
WEP type	*For **Open** authentication type only.* WEP encryption type with a 64-bit or 128-bit key. Select the **WEP-64** value to specify keys containing 5 ASCII symbols or 10 HEX symbols. Select the **WEP-128** value to specify keys containing 13 ASCII symbols or 26 HEX symbols.
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption key WEP as HEX	Move the switch to the right to set a hexadecimal number as a key for encryption.
Encryption key (1-4)	Keys for WEP encryption. The router uses the key selected from the **Default key ID** drop-down list. It is required to specify all the fields. Click the **Show** icon (👁) to display the entered key.

When the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** value is selected, the following fields are displayed on the page:



Security Settings

Network authentication: WPA2-PSK

Password PSK*: ••••••••

Password should be between 8 and 63 ASCII characters

Encryption type*: TKIP

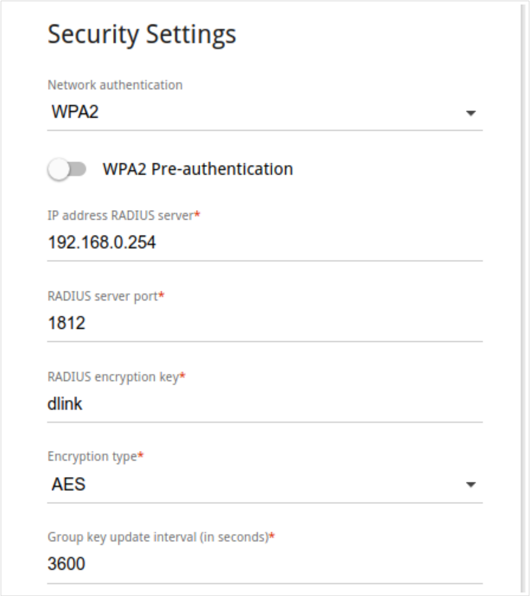
Group key update interval (in seconds)*: 3600

*Figure 98. The **WPA2-PSK** value is selected from the **Network authentication** drop-down list.*

Parameter	Description
Password PSK	A password for WPA encryption. The password can contain digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[12] Click the **Show** icon (👁) to display the entered password.
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**.
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value 0 is specified for this field, the key is not renewed.

[12] 0-9, A-Z, a-z, space, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

When the **WPA**, **WPA2**, or **WPA/WPA2 mixed** value is selected, the following settings are displayed on the page:



Security Settings

Network authentication: WPA2

WPA2 Pre-authentication

IP address RADIUS server*: 192.168.0.254

RADIUS server port*: 1812

RADIUS encryption key*: dlink

Encryption type*: AES

Group key update interval (in seconds)*: 3600

*Figure 99. The **WPA2** value is selected from the **Network authentication** drop-down list.*

Parameter	Description
WPA2 Pre-authentication	Move the switch to the right to activate preliminary authentication (displayed only for the **WPA2** and **WPA/WPA2 mixed** authentication types).
IP address RADIUS server	The IP address of the RADIUS server.
RADIUS server port	A port of the RADIUS server.
RADIUS encryption key	The password which the router uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings).
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**.
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value **0** is specified for this field, the key is not renewed.

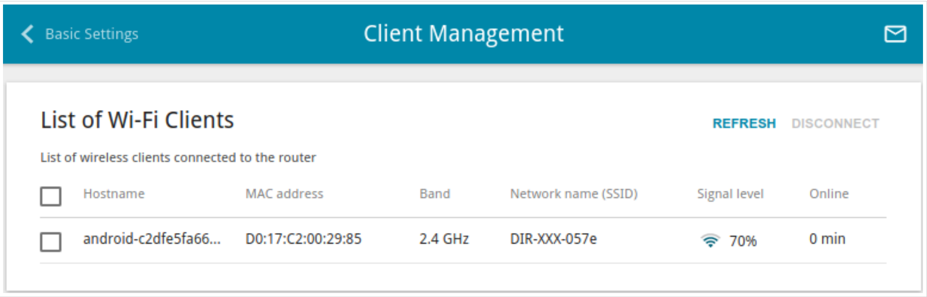
When you have configured the parameters, click the **APPLY** button.

To edit the basic or additional wireless network, left-click the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

To remove the additional network, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button. Then click the **APPLY** button.

Client Management

On the **Wi-Fi / Client Management** page, you can view the list of wireless clients connected to the router.



List of Wi-Fi Clients

List of wireless clients connected to the router

□	Hostname	MAC address	Band	Network name (SSID)	Signal level	Online
□	android-c2dfe5fa66...	D0:17:C2:00:29:85	2.4 GHz	DIR-XXX-057e	70%	0 min

Figure 100. The page for managing the wireless clients.

If you want to disconnect a wireless device from your WLAN, select the checkbox in the line containing the MAC address of this device and click the **DISCONNECT** button.

To view the latest data on the devices connected to the WLAN, click the **REFRESH** button.

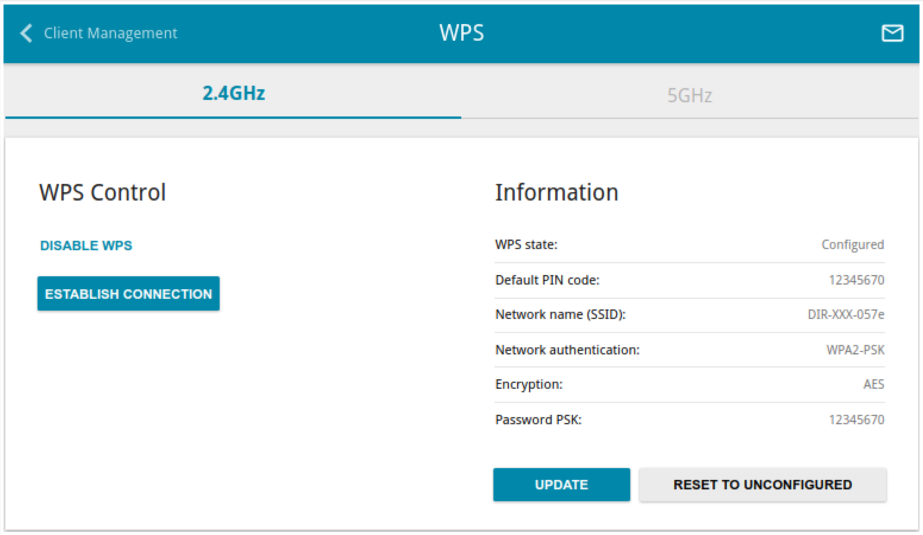
WPS

On the **Wi-Fi / WPS** page, you can enable the function for configuration of the WLAN and select a method for connection to the WLAN.

The WPS function helps to configure the protected wireless network automatically. Devices connecting to the wireless network via the WPS function must support the WPS function.

! The WPS function allows adding devices only to the basic wireless network of the router.

! Before using the function you need to configure one of the following authentication types: **Open** with no encryption, **WPA2-PSK** or **WPA-PSK/WPA2-PSK mixed** with the **AES** encryption method. When other security settings are specified, controls of the **WPS** page on the tab of the relevant band are not available.



WPS state:	Configured
Default PIN code:	12345670
Network name (SSID):	DIR-XXX-057e
Network authentication:	WPA2-PSK
Encryption:	AES
Password PSK:	12345670

Figure 101. The page for configuring the WPS function.

To activate the WPS function, on the tab of the relevant band, click the **ENABLE WPS** button.

When the WPS function is enabled, the **Information** section is available on the page.

Parameter	Description
WPS state	The state of the WPS function: • **Configured** (all needed settings are specified; these settings will be used upon establishing the wireless connection) • **Unconfigured** (after activating the WPS function, the SSID and the encryption key will be configured automatically, the network authentication type will be changed to WPA2-PSK).
Default PIN code	The PIN code of the router. This parameter is used when connecting the router to a registrar to set the parameters of the WPS function.
Network name (SSID)	The name of the router's wireless network.
Network Authentication	The network authentication type specified for the wireless network.
Encryption	The encryption type specified for the wireless network.
Password PSK	The encryption password specified for the wireless network.
UPDATE	Click the button to update the data on the page.
RESET TO UNCONFIGURED	Click the button to reset the parameters of the WPS function.

Using WPS Function via Web-based Interface

To connect to the basic wireless network via the PIN method of the WPS function, follow the next steps:

1. Click the **ENABLE WPS** button.
2. In the **WPS Control** section, click the **ESTABLISH CONNECTION** button.
3. In the opened window, select the **PIN** value from the **WPS method** drop-down list.
4. Select the PIN method in the software of the wireless device that you want to connect to the router's WLAN.
5. Click the relevant button in the software of the wireless device that you want to connect to the WLAN.
6. Right after that, enter the PIN code specified on the cover of the wireless device or in its software in the **PIN code** field.
7. Click the **CONNECT** button in the web-based interface of the router.

To connect to the basic wireless network via the PBC method of the WPS function, follow the next steps:

1. Click the **ENABLE WPS** button.
2. In the **WPS Control** section, click the **ESTABLISH CONNECTION** button.
3. In the opened window, select the **PBC** value from the **WPS method** drop-down list.
4. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
5. Click the relevant button in the software or press the WPS button on the cover of the wireless device that you want to connect to the WLAN.
6. Right after that, click the **CONNECT** button in the web-based interface of the router.

Using WPS Function without Web-based Interface

You can use the WPS function without accessing the web-based interface of the router. To do this, you need to configure the following router's settings:

1. Specify relevant security settings for the wireless network of the router.
2. Click the **ENABLE WPS** button.
3. Save the settings and close the web-based interface (click the **Logout** line of the menu).

Later you will be able to add wireless devices to the WLAN by pressing the **WPS** button of the router.

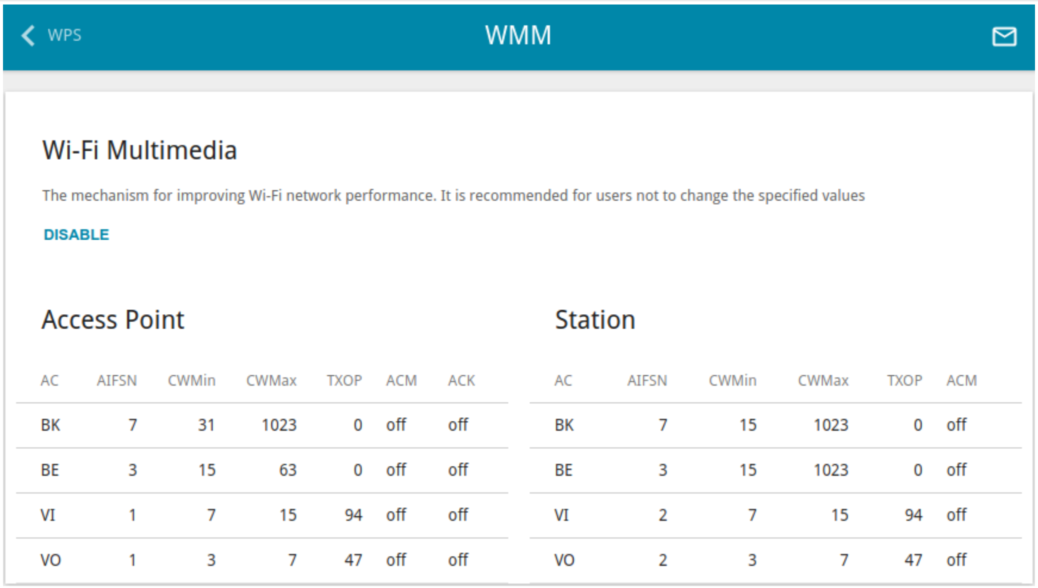
1. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
2. Click the relevant button in the software or press the WPS button on the cover of the wireless device that you want to connect to the WLAN.
3. Press the **WPS** button of the router and release. The **WPS** LED will start blinking.

WMM

On the **Wi-Fi / WMM** page, you can enable the Wi-Fi Multimedia function.

The WMM function implements the QoS features for Wi-Fi networks. It helps to improve the quality of data transfer over Wi-Fi networks by prioritizing different types of traffic.

To enable the function, click the **ENABLE** button. Upon that the **Access Point** and **Station** sections are displayed on the page.



Wi-Fi Multimedia

The mechanism for improving Wi-Fi network performance. It is recommended for users not to change the specified values

DISABLE

Access Point

AC	AIFSN	CWMin	CWMax	TXOP	ACM	ACK
BK	7	31	1023	0	off	off
BE	3	15	63	0	off	off
VI	1	7	15	94	off	off
VO	1	3	7	47	off	off

Station

AC	AIFSN	CWMin	CWMax	TXOP	ACM
BK	7	15	1023	0	off
BE	3	15	1023	0	off
VI	2	7	15	94	off
VO	2	3	7	47	off

Figure 102. The page for configuring the WMM function.

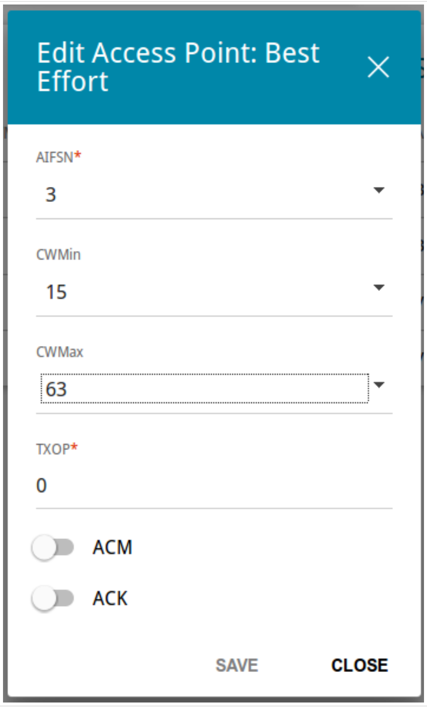
! All needed settings for the WMM function are specified in the device's system. It is recommended not to change the default values.

The WMM function allows assigning priorities for four Access Categories (AC):

- **BK** (*Background*), low priority traffic (print jobs, file downloads, etc.).
- **BE** (*Best Effort*), traffic from legacy devices or devices/applications that do not support QoS.
- **VI** (*Video*).
- **VO** (*Voice*).

Parameters of the Access Categories are defined for both the router itself (in the **Access Point** section) and wireless devices connected to it (in the **Station** section).

To edit the parameters of an Access Category, left-click the relevant line. In the opened window, change the needed parameters.



Edit Access Point: Best Effort

AIFSN*: 3

CWMin: 15

CWMax: 63

TXOP*: 0

ACM

ACK

Figure 103. The window for changing parameters of the WMM function.

Parameter	Description
AIFSN	*Arbitrary Inter-Frame Space Number*. This parameter influences time delays for the relevant Access Category. The lower the value, the higher is the Access Category priority.
CWMin/CWMax	*Contention Window Minimum/Contention Window Maximum*. Both fields influence time delays for the relevant Access Category. The **CWMax** field value should not be lower, than the **CWMin** field value. The lower the difference between the **CWMax** field value and the **CWMin** field value, the higher is the Access Category priority.
TXOP	*Transmission Opportunity*. The higher the value, the higher is the Access Category priority.
ACM	*Admission Control Mandatory*. If the switch is moved to the right, the device cannot use the relevant Access Category.

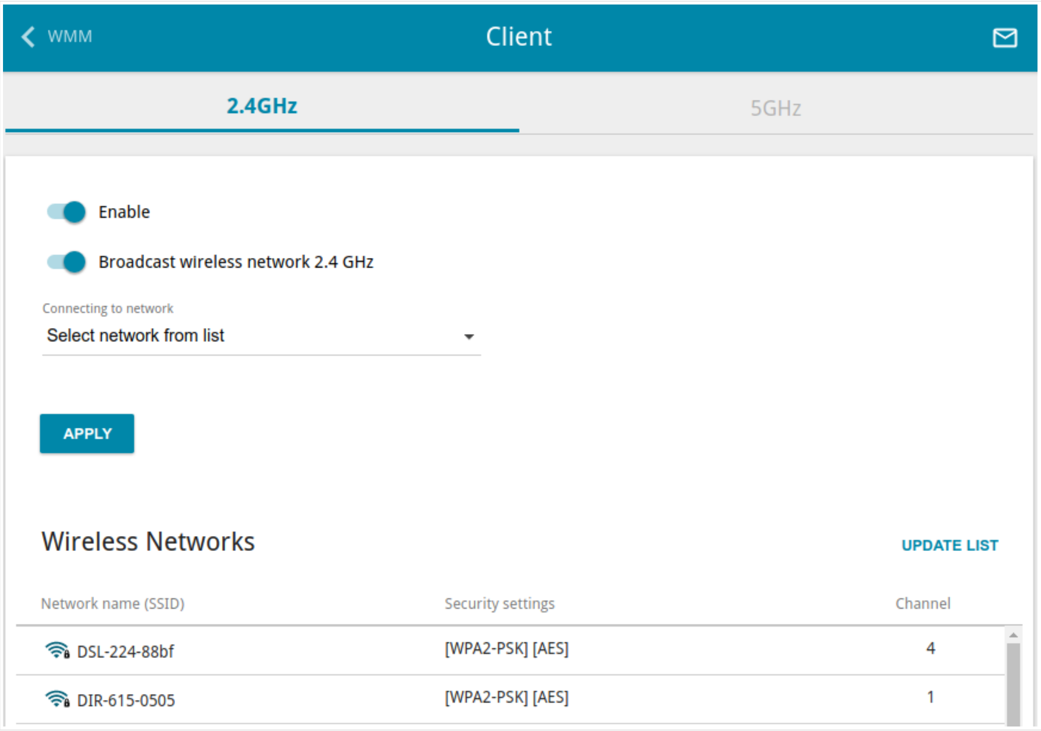
Parameter	Description
ACK	*Acknowledgment*. Answering response requests while transmitting. Displayed only in the **Access Point** section. If the switch is moved to the left, the router answers requests. If the switch is moved to the right, the router does not answer requests.

Click the **SAVE** button.

To disable the WMM function, click the **DISABLE** button.

Client

On the **Wi-Fi / Client** page, you can configure the router as a client to connect to a wireless access point or to a WISP. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.



● Enable

● Broadcast wireless network 2.4 GHz

Connecting to network: Select network from list

Wireless Networks

Network name (SSID)	Security settings	Channel
DSL-224-88bf	[WPA2-PSK] [AES]	4
DIR-615-0505	[WPA2-PSK] [AES]	1

Figure 104. The page for configuring the client mode.

To configure the router as a client, move the **Enable** switch to the right. Upon that the following fields are displayed on the page:

Parameter	Description
Broadcast wireless network 2.4 GHz / Broadcast wireless network 5 GHz	If the switch is moved to the left, devices cannot connect to the router's WLAN. Upon that the router can connect to another access point as a wireless client.
Connecting to network	A method for connecting to another access point.

In the **Wireless Networks** section, the list of available wireless networks is displayed. To view the latest data on available wireless networks, click the **UPDATE LIST** button.

To connect to a wireless network from the list, select the needed network. Move the **Network options** switch to the right to view more detailed information on the network to which the router connects. If a password is required, enter it in the relevant field. Click the **CONNECT** button.

To connect to a hidden network, select the **Connect to hidden network** value from the **Connecting to network** drop-down list. Enter the name of the network in the **Network name (SSID)** field. If needed, fill in the **BSSID** field. Then select the needed type of authentication from the **Network authentication** drop-down list.

When the **Open**, **WEP-64**, or **WEP-128** authentication type is selected, the following settings are displayed on the page:

Parameter	Description
Enable encryption WEP	*For **Open** authentication type only.* To activate WEP encryption, move the switch to the right. Upon that the **WEP type** and **Default key ID** drop-down lists, the **Encryption key WEP as HEX** switch, and four **Encryption key** fields are displayed on the page.
WEP type	*For **Open** authentication type only.* WEP encryption type with a 64-bit or 128-bit key. Select the **WEP-64** value to specify keys containing 5 ASCII symbols or 10 HEX symbols. Select the **WEP-128** value to specify keys containing 13 ASCII symbols or 26 HEX symbols.
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption key WEP as HEX	Move the switch to the right to set a hexadecimal number as a key for encryption.
Encryption key (1-4)	Keys for WEP encryption. The router uses the key selected from the **Default key ID** drop-down list. It is required to specify all the fields. Click the **Show** icon (👁) to display the entered key.

When the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** authentication type is selected, the following fields are displayed:

Parameter	Description
Password PSK	A password for WPA encryption. Click the **Show** icon (👁) to display the entered password.
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**.

When you have configured the parameters, click the **APPLY** button.

When connecting to a wireless access point, the wireless channel of DIR-853 will switch to the channel of the access point to which you have connected.

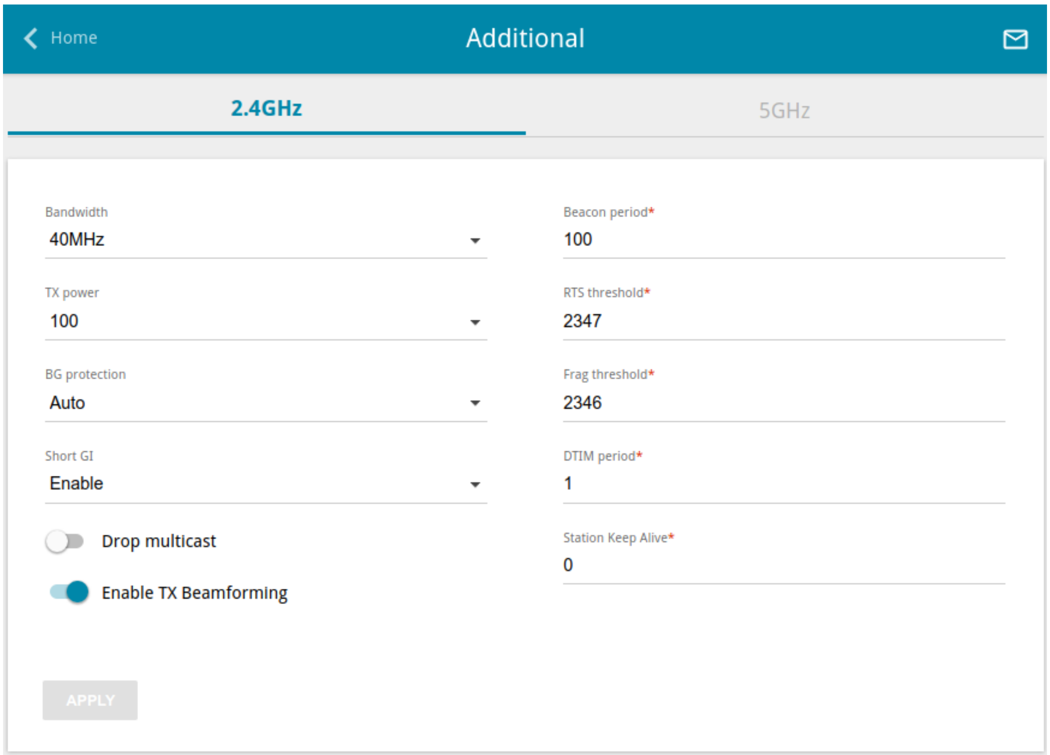
In addition, the **Connection Information** section in which you can view the connection status and the network basic parameters is displayed.

If you want to connect to the WISP network, after configuring the device as a client, you need to create a WAN connection with relevant parameters for the **WiFiClient24ghz** interface in the 2.4GHz band or for the **WiFiClient5ghz** interface in the 5GHz band.

Additional

On page of the **Wi-Fi / Additional** section, you can define additional parameters for the WLAN of the router. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

! Changing parameters presented on this page may negatively affect your WLAN!



Bandwidth: 40MHz
TX power: 100
BG protection: Auto
Short GI: Enable
Drop multicast
Enable TX Beamforming
Beacon period*: 100
RTS threshold*: 2347
Frag threshold*: 2346
DTIM period*: 1
Station Keep Alive*: 0

Figure 105. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
Bandwidth	The channel bandwidth for 802.11n standard in the 2.4GHz band (the **2.4GHz** tab). **20MHz**: 802.11n clients operate at 20MHz channels. **40MHz**: 802.11n clients operate at 40MHz channels. **20/40MHz -**: 802.11n clients operate at 20MHz or 40MHz channels (the channel is combined with the previous adjacent channel). **20/40MHz +**: 802.11n clients operate at 20MHz or 40MHz channels (the channel is combined with the next adjacent channel). The channel bandwidth for 802.11n and 802.11ac standards in 5GHz band (the **5GHz** tab). **20MHz**: 802.11n and 802.11ac clients operate at 20MHz channels. **40MHz**: 802.11n and 802.11ac clients operate at 40MHz channels.

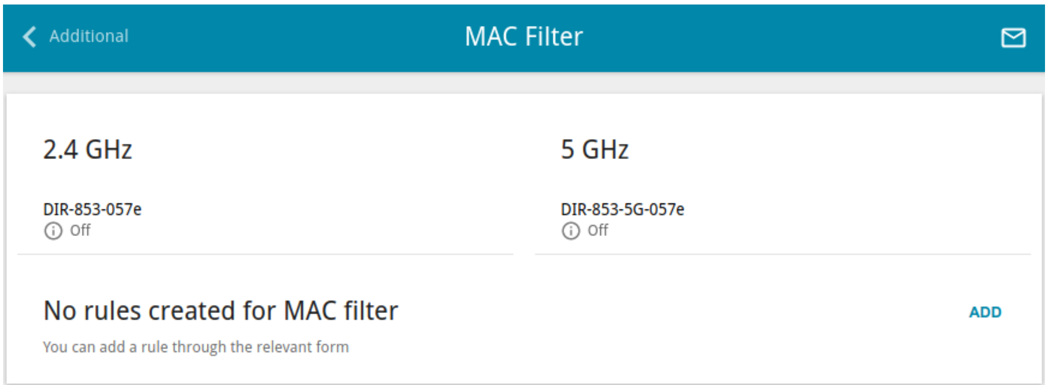
Parameter	Description
	80MHz: 802.11ac clients operate at 80MHz channels.
TX Power	The transmit power (in percentage terms) of the router.
BG protection	*Available on the* ***2.4GHz*** *tab.* The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network. Select a value from the drop-down list. **Auto**: The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices). **Always On**: The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network). **Always Off**: The protection function is always disabled.
Short GI	Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the router is communicating to wireless devices. **Enable**: the router uses the 400 ns short guard interval. Only for the wireless network operating modes which support 802.11n and 802.11ac standards (see the value of the **Wireless mode** drop-down list on the **Wi-Fi / Basic Settings** page). **Disable**: the router uses the 800 ns standard guard interval.
Drop multicast	Move the switch to the right to disable multicasting for the router's WLAN. Move the switch to the left to enable multicasting from the WAN connection selected in the **IGMP** section on the **Connections Setup / WAN** page.
Enable TX Beamforming	TX Beamforming is the signal processing/directing technique which helps to support a high enough transfer rate in the areas with difficult conditions for the signal propagation. Move the switch to the right to improve the signal quality.
Beacon Period	The time interval (in milliseconds) between packets sent to synchronize the wireless network.
RTS threshold	The minimum size (in bytes) of a packet for which an RTS frame is transmitted.
Frag threshold	The maximum size (in bytes) of a non-fragmented packet. Larger packets are fragmented (divided).

Parameter	Description
DTIM period	The time period (in seconds) between sending a DTIM (a message notifying on broadcast or multicast transmission) and data transmission.
Station Keep Alive	The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value 0 is specified, the checking is disabled.

When you have configured the parameters, click the **APPLY** button.

MAC Filter

On the **Wi-Fi / MAC Filter** page, you can define a set of MAC addresses of devices which will be allowed to access the WLAN, or define MAC addresses of devices which will not be allowed to access the WLAN.



Additional

MAC Filter

2.4 GHz

DIR-853-057e
Off

5 GHz

DIR-853-5G-057e
Off

No rules created for MAC filter

You can add a rule through the relevant form

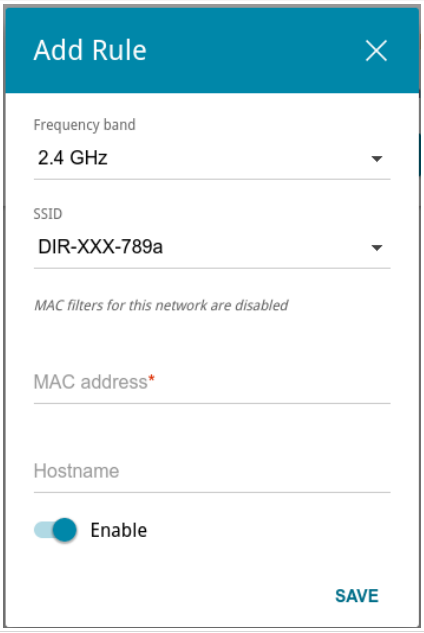
Figure 106. The page for configuring the MAC filter for the wireless network.

By default, MAC filtering is disabled.

To open the basic or additional wireless network of one or both bands for the devices which MAC addresses are specified on this page and to close the wireless network for all other devices, in the section corresponding to the band (**2.4 GHz** or **5 GHz**), left-click the line of the wireless network. In the opened window, move the **Enable MAC filter** switch to the right. Upon that the **MAC filter restrict mode** drop-down list will be displayed. Select the **Allow** value from the drop-down list and click the **SAVE** button.

To close the wireless network for the devices which MAC addresses are specified on this page, select the **Deny** value from the **MAC filter restrict mode** drop-down list and click the **SAVE** button.

Click the **ADD** button to add a rule for MAC filtering.



Add Rule

Frequency band: 2.4 GHz

SSID: DIR-XXX-789a

MAC filters for this network are disabled

MAC address*

Hostname

Enable

Figure 107. The window for adding a rule for the MAC filter.

You can specify the following parameters:

Parameter	Description
Frequency band	From the drop-down list, select a band of the wireless network.
SSID	A wireless network to which the rule will be applied. Select the needed value from the drop-down list.
MAC address	In the field, enter the MAC address to which the selected filtering mode will be applied.
Hostname	The name of the device for easier identification. You can specify any name.
Enable	If the switch is moved to the right, the rule is active. Move the switch to the left to disable the rule.

When you have configured the parameters, click the **SAVE** button.

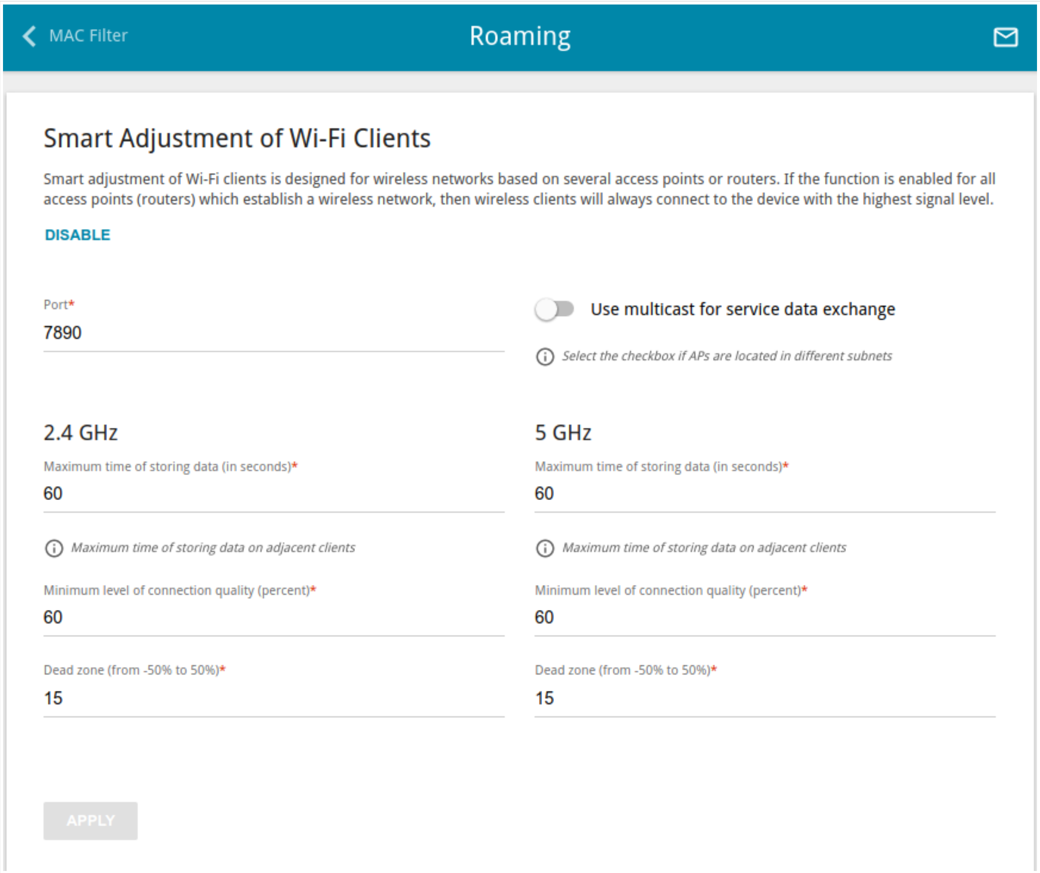
To edit the parameters of the existing rule, in the **Filters** section, left-click the needed rule. In the opened window, change the settings and click the **SAVE** button.

To remove the rule from the page, in the **Filters** section, select the checkbox located to the left of the relevant rule and click the **DELETE** button.

Roaming

On the **Wi-Fi / Roaming** page, you can enable the function of smart adjustment of Wi-Fi clients.

This function is designed for wireless networks based on several access points or routers. If the function is enabled for all access points (routers) which establish a wireless network, then wireless clients will always connect to the device with the highest signal level.



Smart Adjustment of Wi-Fi Clients

Smart adjustment of Wi-Fi clients is designed for wireless networks based on several access points or routers. If the function is enabled for all access points (routers) which establish a wireless network, then wireless clients will always connect to the device with the highest signal level.

DISABLE

Port*: 7890

Use multicast for service data exchange

Select the checkbox if APs are located in different subnets

2.4 GHz

Maximum time of storing data (in seconds)*: 60

Maximum time of storing data on adjacent clients

Minimum level of connection quality (percent)*: 60

Dead zone (from -50% to 50%)*: 15

5 GHz

Maximum time of storing data (in seconds)*: 60

Maximum time of storing data on adjacent clients

Minimum level of connection quality (percent)*: 60

Dead zone (from -50% to 50%)*: 15

APPLY

*Figure 108. The **Wi-Fi / Roaming** page.*

To enable the function, click the **ENABLE** button. Upon that the following settings are available on the page.

Parameter	Description
Port	The number of the port used for data exchange between access points (routers).
Use multicast for service data exchange	Move the switch to the right in order to use multicast traffic for service data exchange between access points (routers). This setting is needed if the devices which support the smart adjustment function are located in different subnets. If the switch is moved to the right, the **Multicast TTL** and **Multicast group address** fields are displayed on the page. If the switch is moved to the left, broadcast traffic is used for service data exchange.

Parameter	Description
Multicast TTL	Specify the TTL (*Time to live*) parameter value. The recommended value is `4`.
Multicast group address	Specify the address of the multicast group (from the subnet 239.255.0.0/16).
2.4 GHz / 5 GHz	
Maximum time of storing data	The maximum time period (in seconds) during which the access point (router) stores data on the signal strength of the client located on its coverage area.
Minimum level of connection quality	The threshold value of the signal strength upon which the access point (router) starts scanning other devices.
Dead zone	This parameter is used for calculation of the signal strength upon which the smart adjustment function goes off. If the signal strength provided by the device is less than the sum of the **Minimum level of connection quality** field value and the **Dead zone** field value, then the client disconnects from the access point (router) and connects to another device. You can specify the values from `-50%` to `+50%`.

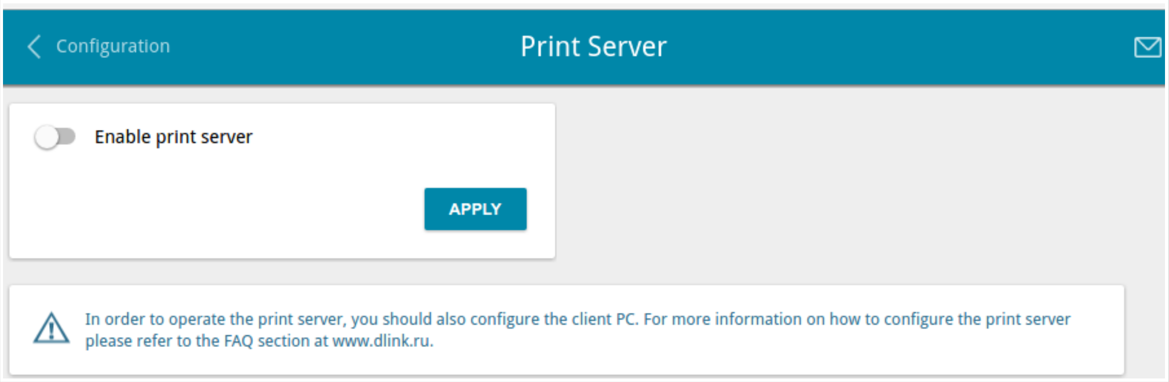
After specifying the needed parameters, click the **APPLY** button.

To disable the function of smart adjustment of Wi-Fi clients, click the **DISABLE** button.

Print Server

On the **Print Server** page, you can configure the router as a print server. Being configured in this way, the router will allow your LAN users to share the printer connected to the USB port of the router.

To connect a printer to the router, power off both devices. Connect the printer to the USB port of the router, power on the printer, then power on the router.



In order to operate the print server, you should also configure the client PC. For more information on how to configure the print server please refer to the FAQ section at www.dlink.ru.

*Figure 109. The **Print Server** page.*

To configure the router as a print server, move the **Enable print server** switch to the right and click the **APPLY** button.

If you don't want to use the router as a print server, move the **Enable print server** switch to the left and click the **APPLY** button.

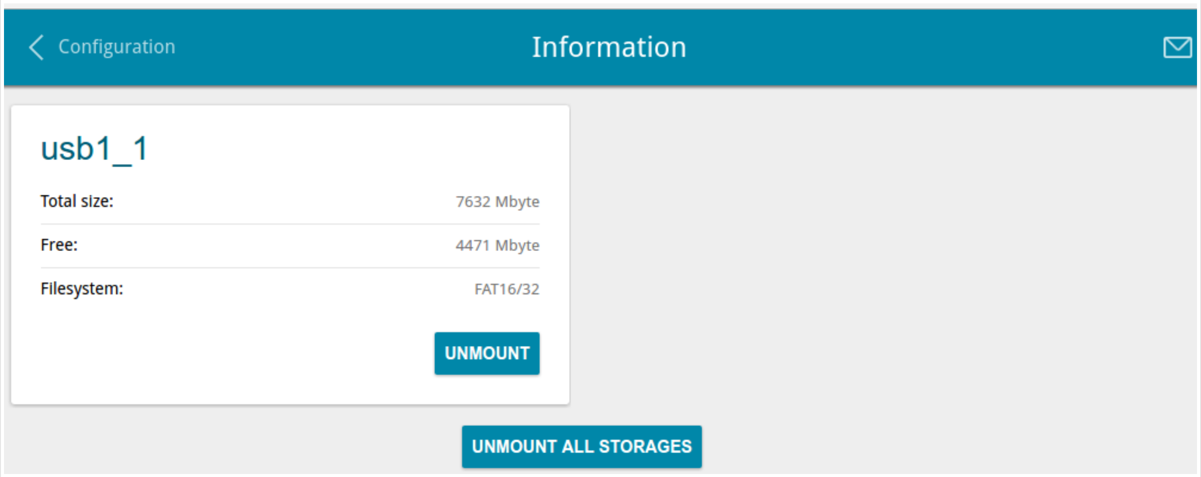
USB Storage

This menu is designed to operate USB storages. Here you can do the following:

- view data on the connected USB storage
- create accounts for users to allow access to the content of the USB storage
- enable the built-in Samba server of the router
- enable the built-in FTP server of the router
- view content of the connected USB storage
- enable the built-in DLNA server of the router
- configure the built-in Transmission torrent client and manage distributing and downloading processes
- enable the XUPNPD plug-in.

Information

On the **USB Storage / Information** page, you can view data on the USB storage connected to the router.



Total size:	7632 Mbyte
Free:	4471 Mbyte
Filesystem:	FAT16/32

*Figure 110. The **USB Storage / Information** page.*

The following data are presented on the page: the name, total and free space of the storage, and the type of its file system (supported file systems: FAT16/32, NTFS, and ext2/3).

If the USB storage is divided into volumes, a section for every volume (partition) of the USB storage is displayed on the page.

To safely disconnect the USB storage or a volume of the USB storage, click the **UNMOUNT** button in the relevant section and wait for several seconds.

To disconnect all volumes of the USB storage, click the **UNMOUNT ALL STORAGES** button.

USB Users

On the **USB Storage / USB Users** page, you can create user accounts to provide access to data on the USB storage connected to the router.

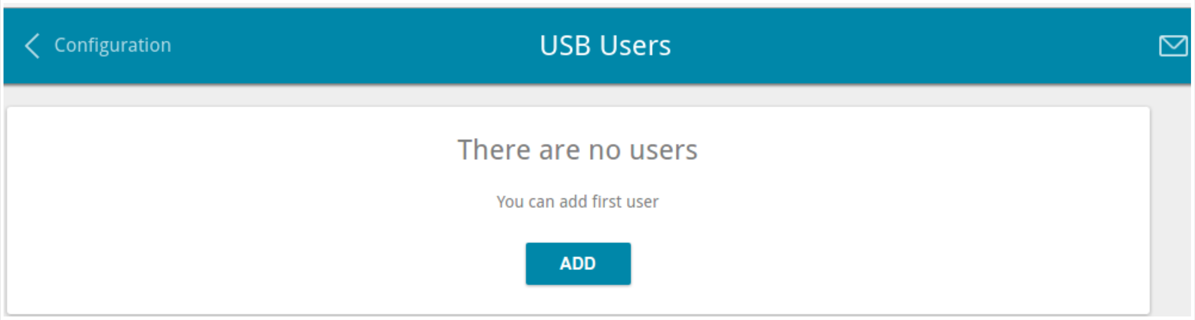


*Figure 111. The **USB Storage / USB users** page.*

To create a new user account, click the **ADD** button.

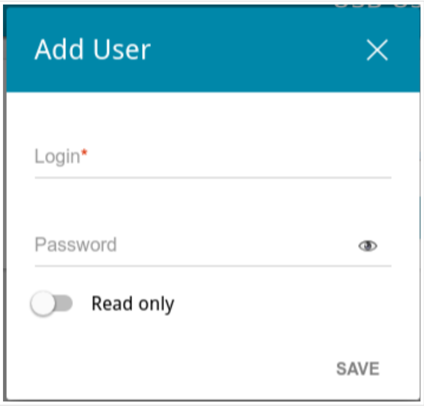


Figure 112. The window for adding a user.

In the opened window, in the **Login** field, specify a username, and in the **Password** field – the password for the account. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[13]

! You cannot create accounts with the following usernames: `admin`, `support`, `user`, `nobody`.

For ext2, ext3, or FAT storages or storage partitions, it is possible to create users with limited rights. Move the **Read only** switch to the right not to let the user create, change, or delete files.

Click the **SAVE** button.

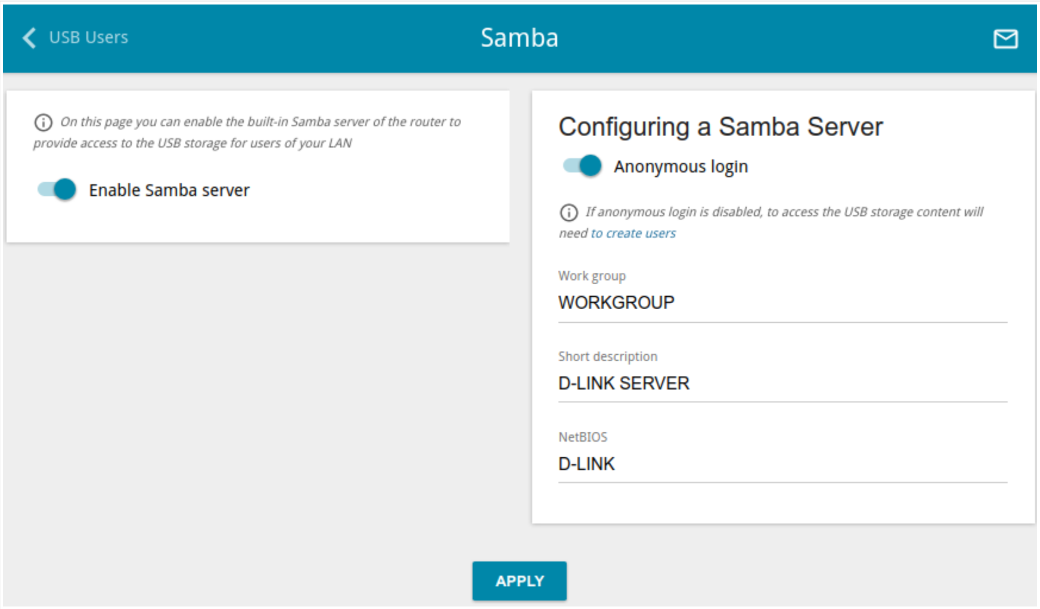
To change the password of an account, select the relevant line in the table. In the opened window, enter a new value in the **Password** field, and then click the **SAVE** button.

To remove an account, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button.

[13] 0-9, A-Z, a-z, space, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

Samba

On the **USB Storage / Samba** page, you can enable the built-in Samba server of the router to provide access to the USB storage for users of your LAN.



On this page you can enable the built-in Samba server of the router to provide access to the USB storage for users of your LAN

Enable Samba server

Configuring a Samba Server

Anonymous login

If anonymous login is disabled, to access the USB storage content will need to create users

Work group: WORKGROUP

Short description: D-LINK SERVER

NetBIOS: D-LINK

*Figure 113. The **USB Storage / Samba** page.*

To enable the Samba server, move the **Enable Samba server** switch to the right.

The **Anonymous login** switch (by default, the switch is moved to the right) allows anonymous access to the content of the USB storage for users of your LAN.

If you want to provide authorized access to the content of the USB storage for users of your LAN, move the switch to the left. After applying the parameters on this page, go to the **USB Storage / USB Users** page and create needed accounts.

In the **Work group** field, leave the value specified by default (**`WORKGROUP`**) or specify a new name of a workgroup which participants will have access to the content of the USB storage.

In the **Short description** field, you can specify an additional description for the USB storage. This value will be displayed in some operating systems. Use digits and/or Latin characters.

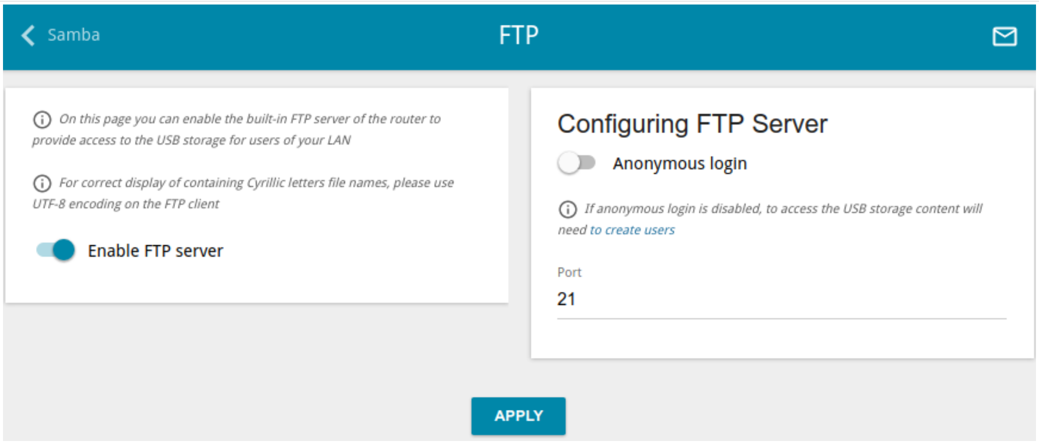
In the **NetBIOS** field, specify a new name of the USB storage for identification in your LAN. Use digits and/or Latin characters.

After specifying the needed parameters, click the **APPLY** button.

To disable the built-in Samba server of the router, move the **Enable Samba server** switch to the left and click the **APPLY** button.

FTP

On the **USB Storage / FTP** page, you can enable the built-in FTP server of the router to provide access to the USB storage for users of your LAN.



On this page you can enable the built-in FTP server of the router to provide access to the USB storage for users of your LAN

For correct display of containing Cyrillic letters file names, please use UTF-8 encoding on the FTP client

● Enable FTP server

Configuring FTP Server

○ Anonymous login

If anonymous login is disabled, to access the USB storage content will need to create users

Port
21

*Figure 114. The **USB Storage / FTP** page.*

To enable the FTP server, move the **Enable FTP server** switch to the right.

Move the **Anonymous login** switch to the right to allow anonymous access to the content of the USB storage for users of your LAN. If you want to provide authorized access to the content of the USB storage for users of your LAN, move the switch to the left. After applying the parameters on this page, go to the **USB Storage / USB Users** page and create needed accounts.

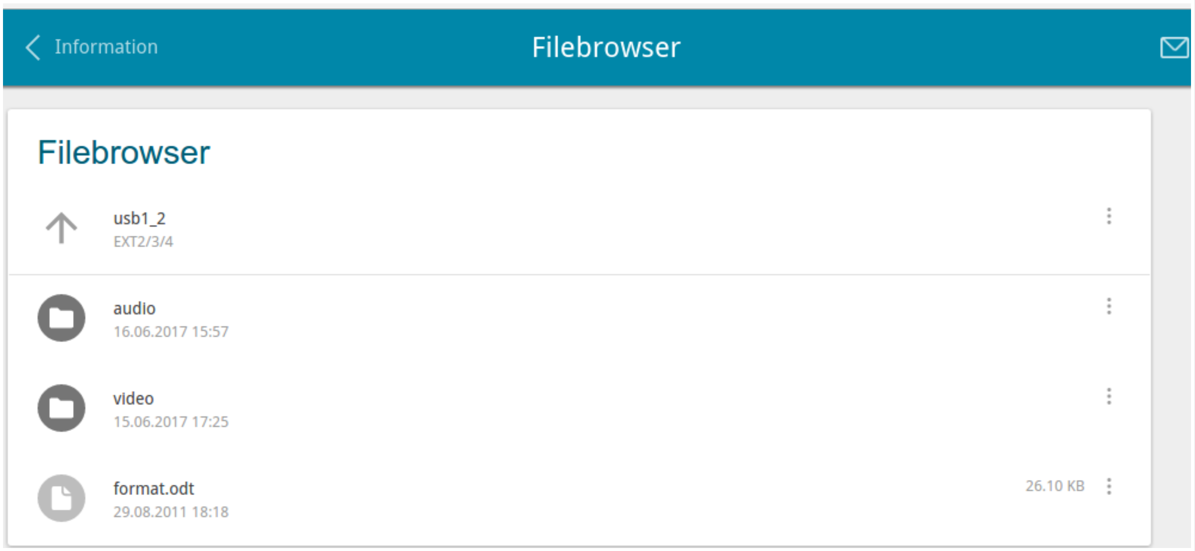
If needed, change the router's port used by the FTP server in the **Port** field (by default, the standard port `21` is specified).

After specifying the needed parameters, click the **APPLY** button.

To disable the built-in FTP server of the router, move the **Enable FTP server** switch to the left and click the **APPLY** button.

Filebrowser

On the **USB Storage / Filebrowser** page, you can view the content of your USB storage connected to the router and remove separate folders and files from the USB storage.



Filebrowser

usb1_2
EXT2/3/4

audio
16.06.2017 15:57

video
15.06.2017 17:25

format.odt
29.08.2011 18:18
26.10 KB

*Figure 115. The **USB Storage / Filebrowser** page.*

To view the content of the USB storage, click the icon of the storage or storage partition. The list of folders and files will be displayed on the page.

To go to a folder, click the line corresponding to this folder.

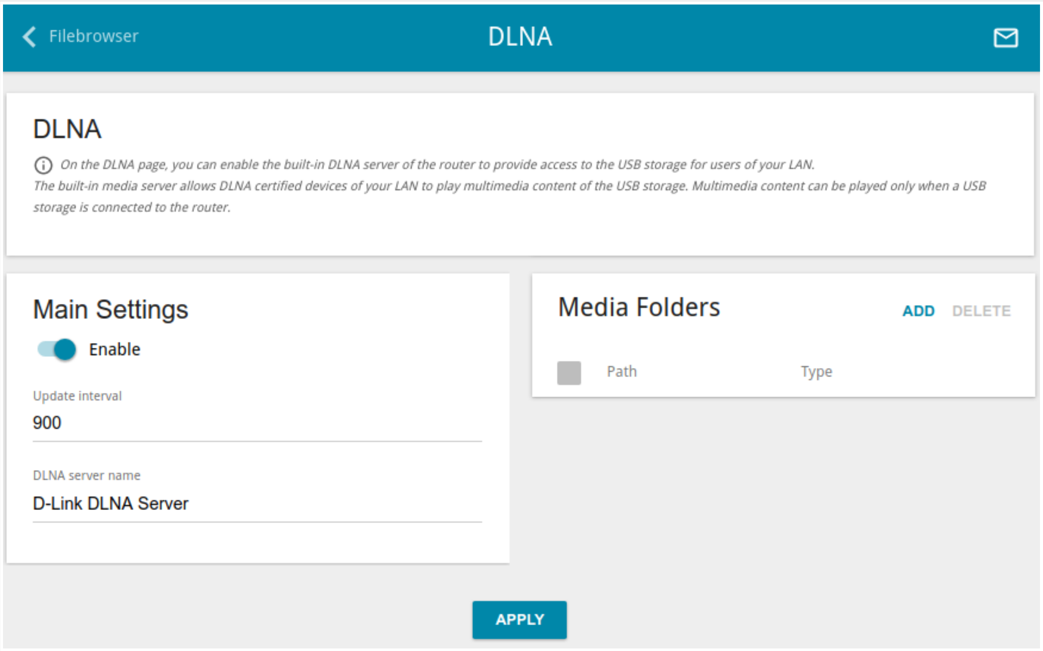
To refresh the folder contents, click the **Actions** icon (⋮) in the line corresponding to this folder and select the **Refresh** value.

To remove a folder or file, click the **Actions** icon (⋮) in the line corresponding to this folder or file and select the **Remove** value.

DLNA

On the **USB Storage / DLNA** page, you can enable the built-in DLNA server of the router to provide access to the USB storage for users of your LAN.

The built-in media server allows DLNA certified devices of your LAN to play multimedia content of the USB storage. Multimedia content can be played only when a USB storage is connected to the router.



DLNA

On the DLNA page, you can enable the built-in DLNA server of the router to provide access to the USB storage for users of your LAN. The built-in media server allows DLNA certified devices of your LAN to play multimedia content of the USB storage. Multimedia content can be played only when a USB storage is connected to the router.

Main Settings

Enable

Update interval: 900

DLNA server name: D-Link DLNA Server

Media Folders

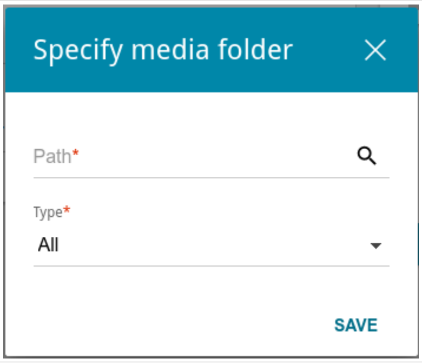
*Figure 116. The **USB Storage / DLNA** page.*

To enable the DLNA server, move the **Enable** switch to the right.

In the **Update interval** field, specify the time period (in seconds), at the end of which the media server updates the file list of the USB storage, or leave the value specified by default (`900`).

In the **DLNA server name** field, specify a new name of the DLNA server for easier identification in your LAN or leave the value specified by default (`D-Link DLNA Server`). Use digits and/or Latin characters.

To allow access to the content of the USB storage for users of your LAN, click the **ADD** button in the **Media Folders** section.



Specify media folder

Path*

Type*
All

Figure 117. Specifying a media folder.

In the opened window, locate a folder containing files. To do this, click the **Search** icon (🔍) in the **Path** field. Then go to the needed folder and click the **SELECT** button.

For each folder you can define the type of files which will be available for users of your LAN. To do this, select the needed type of files from the **Type** drop-down list. To share all files of a folder, select the **All** value from the **Type** drop-down list.

Click the **SAVE** button.

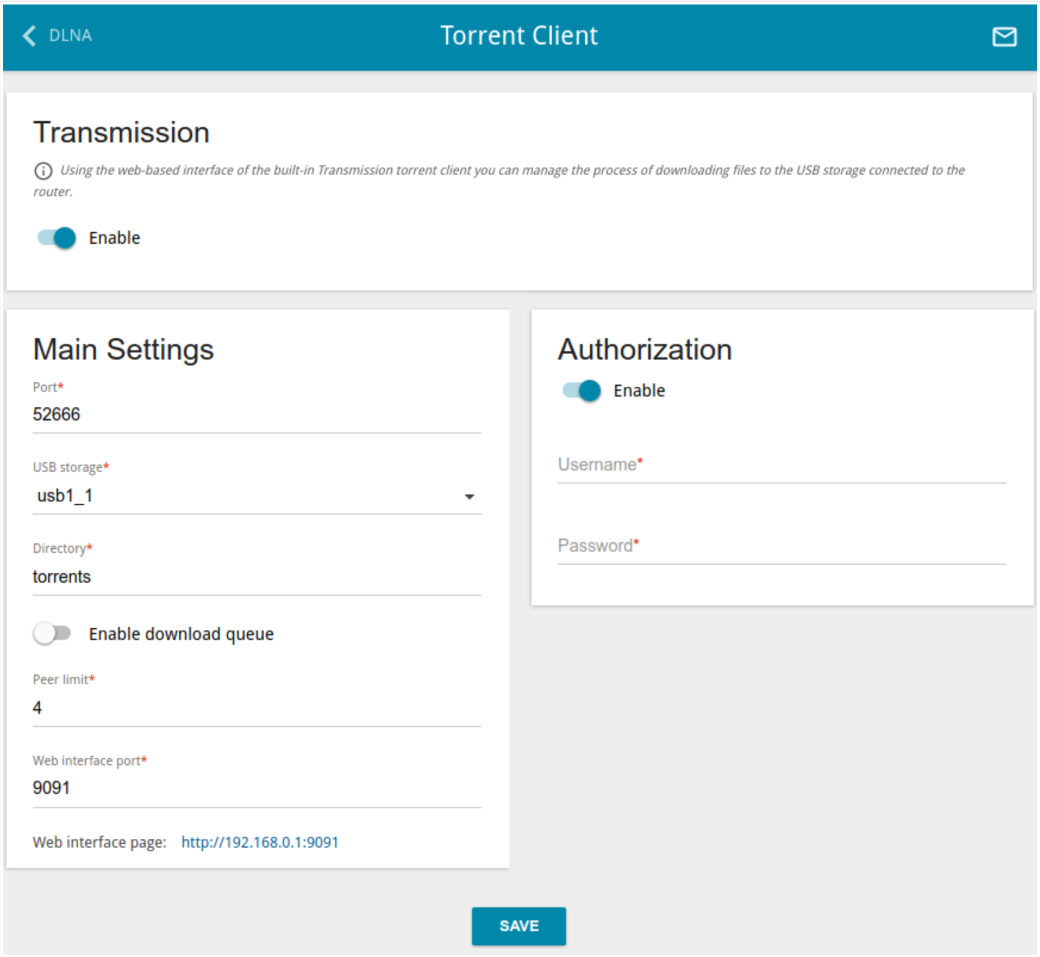
To remove a folder from the list in the **Media Folders** section, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button.

After specifying all needed settings on the **USB Storage / DLNA** page, click the **APPLY** button.

To disable the built-in DLNA server of the router, move the **Enable** switch to the left and click the **APPLY** button.

Torrent Client

On the **USB Storage / Torrent Client** page, you can configure all needed settings for the built-in Transmission client.



Transmission

Using the web-based interface of the built-in Transmission torrent client you can manage the process of downloading files to the USB storage connected to the router.

Enable

Main Settings

Port*: 52666

USB storage*: usb1_1

Directory*: torrents

Enable download queue

Peer limit*: 4

Web interface port*: 9091

Web interface page: http://192.168.0.1:9091

Authorization

Enable

Username*

Password*

*Figure 118. The **USB Storage / Torrent Client** page.*

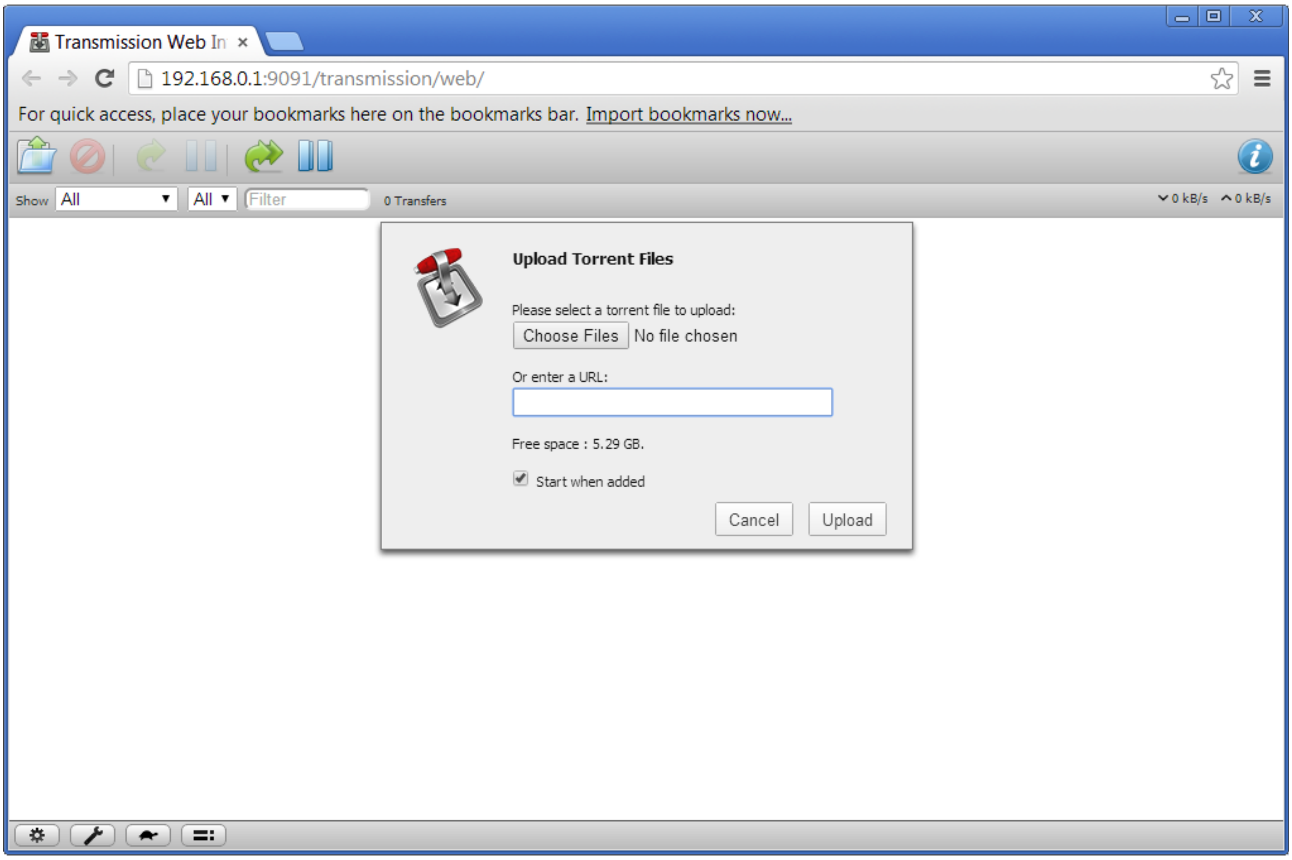
You can specify the following parameters:

Parameter	Description
Transmission	
Enable	Move the switch to the right to activate the Transmission client.
Main Settings	
Port	The router's port which will be used by the Transmission client.
USB storage	From the drop-down list, select a USB storage or a volume.
Directory	The folder on the USB storage where data of the Transmission client will be stored.

Parameter	Description
Enable download queue	Move the switch to the right if you want to limit the number of simultaneous downloads. Upon that the **Download queue size** field will be displayed. Move the switch to the left not to limit the number of simultaneous downloads.
Download queue size	The maximum number of simultaneous downloads. By default, the value **1** is specified.
Peer limit	The maximum number of the service users from which you can download files.
Web interface port	The port on which the web-based interface of the Transmission client is available.
Authorization	
Enable	Move the switch to the right if you want the Transmission client to request for username and password when accessing its web-based interface. Then fill in the **Username** and **Password** fields.
Username	The username to access the web-based interface of the Transmission client.
Password	The password to access the web-based interface of the Transmission client.

After specifying the needed parameters, click the **APPLY** button.

In the **Web-interface page** field, the address of the web-based interface of the Transmission client is displayed. To access the web-based interface of the Transmission client, click the link.



Transmission Web In ×
192.168.0.1:9091/transmission/web/
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Show All ▾ All ▾ Filter 0 Transfers
0 kB/s 0 kB/s

Upload Torrent Files

Please select a torrent file to upload:

Choose Files No file chosen

Or enter a URL:

Free space : 5.29 GB.

☑ Start when added

Cancel Upload

Figure 119. The web-based interface of the Transmission torrent client.

Using the web-based interface of the built-in Transmission torrent client you can manage the process of downloading files to the USB storage connected to the router.

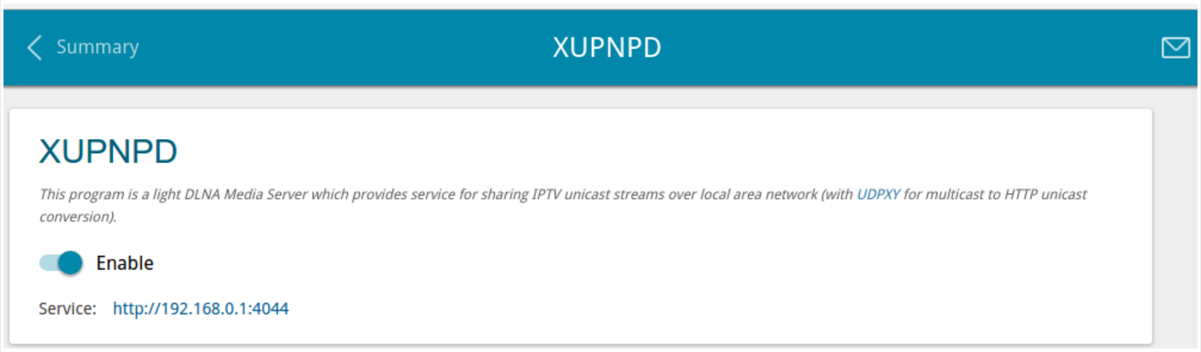
The following buttons are available on the page:

Parameter	Description
Open Torrent	Click the button to add a new torrent file (a metadata file according to which the Transmission client downloads files) to the download queue. In the dialog box appeared, select a file stored on your PC and click the **Upload** button.
Remove Selected Torrents	Select the torrent file which you want to remove from the download queue and click the button.
Start Selected Torrents	Select the torrent file corresponding to the download which should be restarted and click the button.

Parameter	Description
Start All Torrents	Click the button to restart all downloads. If you limited the maximum number of simultaneous downloads, the Transmission client starts processing of the specified number of torrent files; after completing download of the first one, the client proceeds to the next file in the queue.
Pause Selected Torrents	Select the torrent file corresponding to the download which should be stopped and click the button.
Pause All Torrents	Click the button to stop all downloads.
Toggle Inspector	Select a torrent file and click the button to view its data.

XUPNPD

On the **USB Storage / XUPNPD** page, you can enable the XUPNPD plug-in. It allows to broadcast media content received from the Internet sources or IPTV service to DLNA-certified devices of your LAN.



XUPNPD

This program is a light DLNA Media Server which provides service for sharing IPTV unicast streams over local area network (with UDPXY for multicast to HTTP unicast conversion).

● Enable

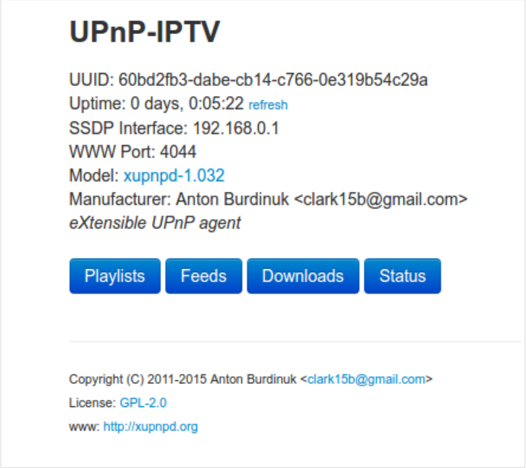
Service: http://192.168.0.1:4044

*Figure 120. The **USB Storage / XUPNPD** page.*

To use the XUPNPD plug-in, connect a USB storage to the router and move the **Enable** switch to the right.

! To let IPTV services operate using the XUPNPD plug-in, enable the UDPXY application.

In the **Service** field, the address of the web-based interface of the XUPNPD plug-in is displayed. To access the page of the XUPNPD plug-in and configure all needed settings, click the link.



UPnP-IPTV

UUID: 60bd2fb3-dabe-cb14-c766-0e319b54c29a
Uptime: 0 days, 0:05:22 refresh
SSDP Interface: 192.168.0.1
WWW Port: 4044
Model: xupnpd-1.032
Manufacturer: Anton Burdinuk <clark15b@gmail.com>
eXtensible UPnP agent

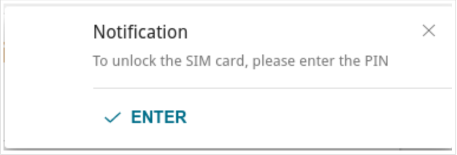
Copyright (C) 2011-2015 Anton Burdinuk <clark15b@gmail.com>
License: GPL-2.0
www: http://xupnpd.org

Figure 121. The XUPNPD plug-in page.

USB Modem

This menu is designed to operate USB modems.

If the PIN code check for the SIM card inserted into your USB modem is not disabled, the relevant notification will be displayed in the top right corner of the page.

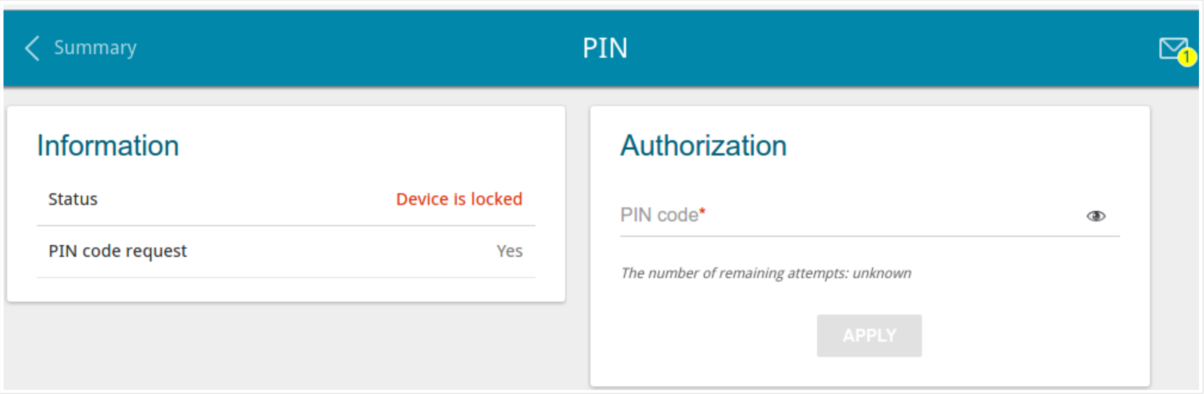


Notification

To unlock the SIM card, please enter the PIN

Figure 122. The notification on the PIN code check.

Click the **ENTER** button. When the **USB Modem / PIN** page opens, enter the PIN code in the **Authorization** section[14]. Click the **Show** icon (👁) to display the entered code. Then click the **APPLY** button.



Information

Status	Device is locked
PIN code request	Yes

Authorization

PIN code*

The number of remaining attempts: unknown

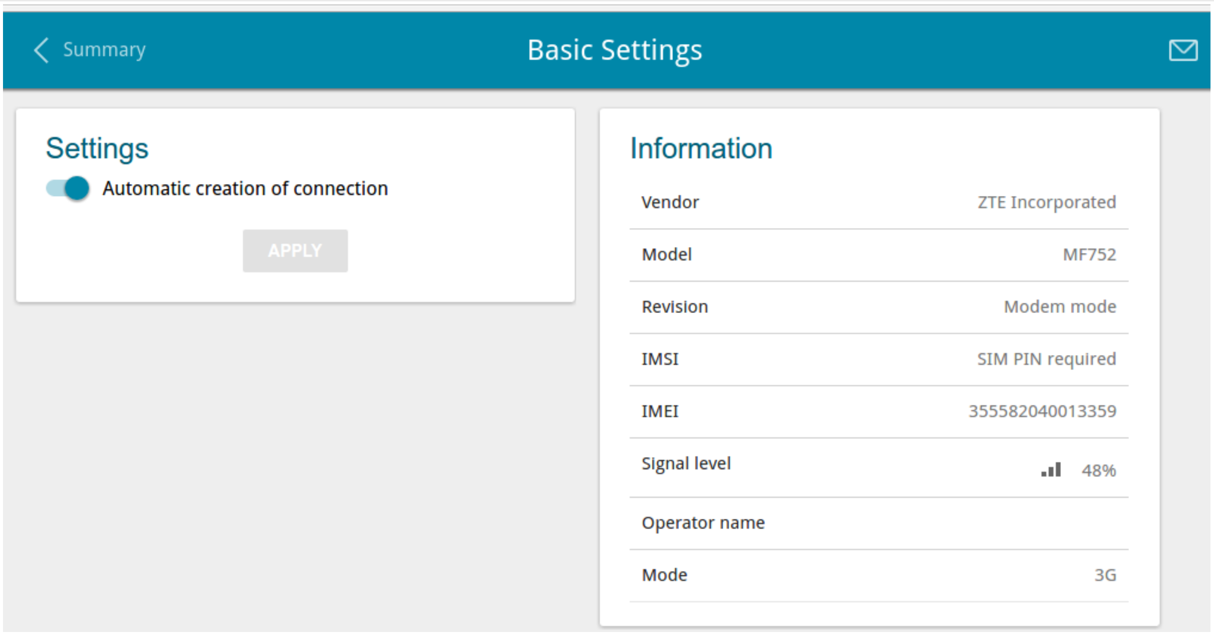
Figure 123. Entering the PIN code.

Some USB modems in the router mode and Android smartphones in the modem mode have an IP address from the subnet which coincides with the router's local subnet. In this case, the router's web-based interface can be unavailable. For correct operation, disconnect the device from the USB port and reboot the router. Then access the web-based interface, go to the **Connections Setup / LAN** page, and change the value of the **IP address** field on the **IPv4** tab (for example, specify the value `192.168.2.1`). Wait until the router is rebooted.

[14] For some models of LTE USB modems it is required to disable the PIN code check on the SIM card prior to connecting the USB modem to the router.

Basic Settings

On the **USB Modem / Basic Settings** page, you can view data on the USB modem connected to the router and enable/disable the function for automatic creation of 3G/LTE WAN connection upon plugging a USB modem into the router.



Vendor	ZTE Incorporated
Model	MF752
Revision	Modem mode
IMSI	SIM PIN required
IMEI	355582040013359
Signal level	48%
Operator name	
Mode	3G

*Figure 124. The **USB Modem / Basic Settings** page.*

If the **Automatic creation of connection** switch is moved to the right and the PIN code check for the SIM card inserted into your USB modem is disabled, then an active WAN connection with default settings (for LTE modems) or the operator's settings (for GSM modems) will be automatically created when plugging the USB modem into the router. The connection will be displayed on the **Connections Setup / WAN** page.

If you don't want to use this function, move the **Automatic creation of connection** switch to the right and click the **APPLY** button.

When a USB modem is connected to the router, the following data are displayed in the **Information** section:

Parameter	Description
Vendor	The manufacturer of your USB modem.
Model	The alphanumeric code of the model of your USB modem.
Revision	The revision of the firmware of your USB modem.
IMSI	The code stored in the SIM card inserted to your USB modem.
IMEI	The code stored in the memory of the USB modem.

Parameter	Description
Signal level	The signal level at the input of the modem's receiver. The zero signal level shows that you are out of the coverage area of the selected operator's network.
Operator name	When the needed network is available, the name of the operator is displayed in this field.
Mode	A type of the network to which the USB modem is connected.

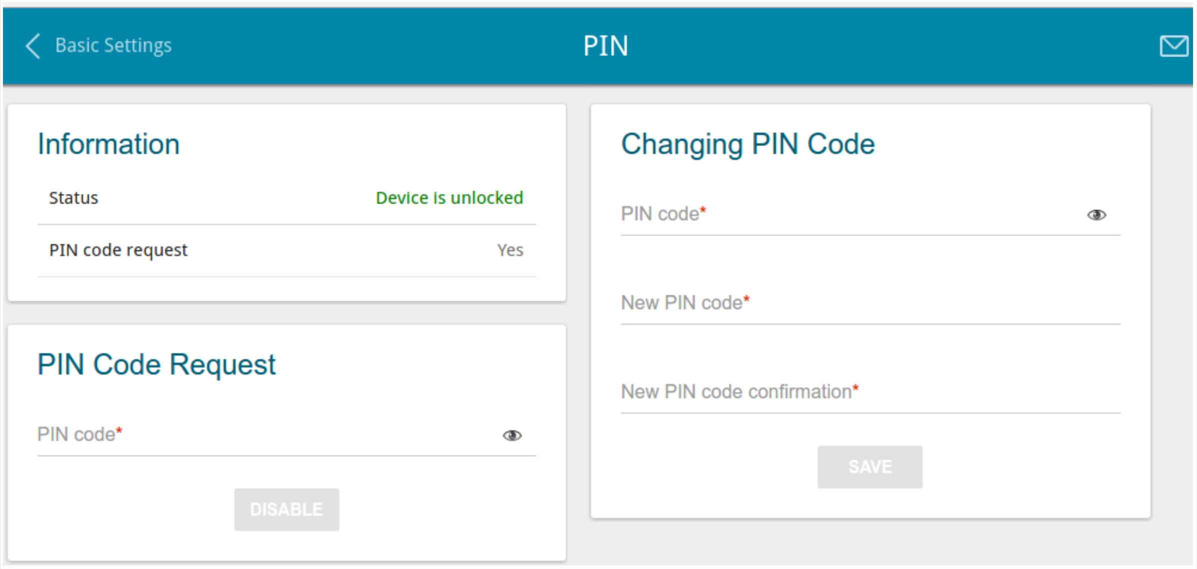
PIN

On the **USB Modem / PIN** page, you can change the PIN code of the SIM card inserted into your USB modem, disable or enable the check of the PIN code.

! The operations presented on this page are unavailable for some models of LTE USB modems.

The current state of the SIM card inserted into your USB modem is displayed in the **Status** field. If the PIN code is entered incorrectly or the PIN code is not entered when the PIN code check is enabled, the **Device is locked** value is displayed in the **Status** field. If the PIN code is entered correctly or the PIN check is disabled, the **Device is unlocked** value is displayed in the **Status** field.

If the PIN code check for the SIM card inserted into your USB modem is not disabled, the **Yes** value is displayed in the **PIN code request** field. If the PIN check is disabled, the **No** value is displayed in the **PIN code request** field.



Status	Device is unlocked
PIN code request	Yes

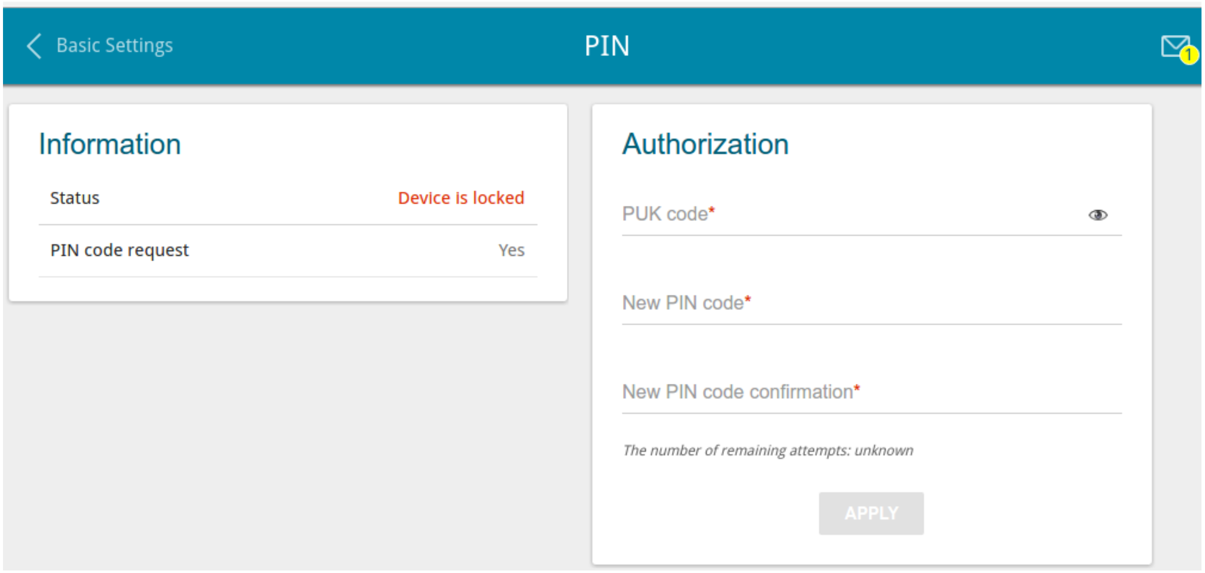
*Figure 125. The **USB Modem / PIN** page.*

To disable the PIN code check, in the **PIN Code Request** section, enter the current PIN code in the **PIN code** field and click the **DISABLE** button (the button is displayed if the PIN code check is enabled).

To enable the PIN code check, in the **PIN Code Request** section, enter the PIN code used before disabling the check in the **PIN code** field and click the **ENABLE** button (the button is displayed if the PIN code check is disabled).

To change the PIN code, in the **Changing PIN Code** section, enter the current code in the **PIN code** field, then enter a new code in the **New PIN code** and **New PIN code confirmation** fields and click the **SAVE** button.

If upon one of the operations described above you have entered an incorrect value in the **PIN code** field three times (the number of remaining attempts is displayed on the page), the SIM card inserted into your USB modem is blocked.



Information

Status	Device is locked
PIN code request	Yes

Authorization

PUK code*

New PIN code*

New PIN code confirmation*

The number of remaining attempts: unknown

*Figure 126. The **USB Modem / PIN** page. The PUK code request.*

For further use of the card, in the **Authorization** section, enter the PUK code in the relevant field, and then specify a new PIN code for your SIM card in the **New PIN code** and **New PIN code confirmation** field. Click the **APPLY** button.

Advanced

In this menu you can configure advanced settings of the router:

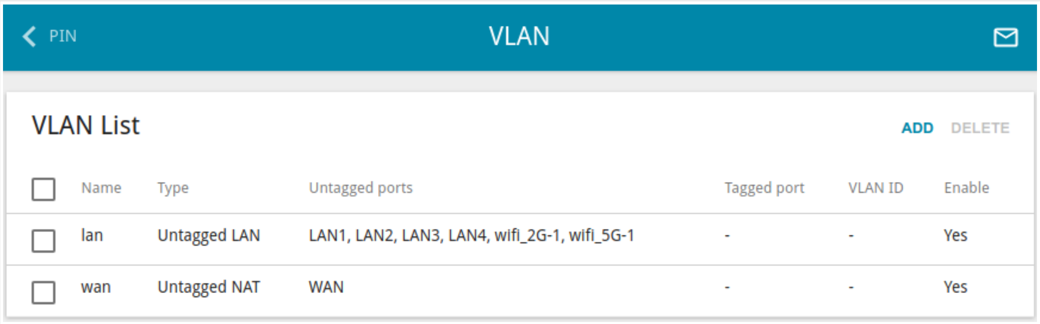
- create groups of ports for VLANs
- add name servers
- configure the SafeDNS or SkyDNS service
- configure a DDNS service
- configure notifications on the reason of the Internet connection failure
- define static routes
- configure TR-069 client
- create rules for remote access to the web-based interface
- enable the UPnP IGD protocol
- enable the built-in UDPXY application for the router
- allow the router to use IGMP, RTSP, enable the SIP ALG, the PPPoE/PPTP/L2TP/IPsec pass through functions for the router
- configure VPN tunnels based on IPsec protocol.

VLAN

On the **Advanced / VLAN** page, you can create and edit groups of ports for virtual networks (VLANs).

By default, 2 groups are created in the router's system:

- **lan**: it includes ports 1-4. You cannot delete this group.
- **wan**: for the WAN interface; it includes the **INTERNET** port. You can edit or delete this group.



VLAN List

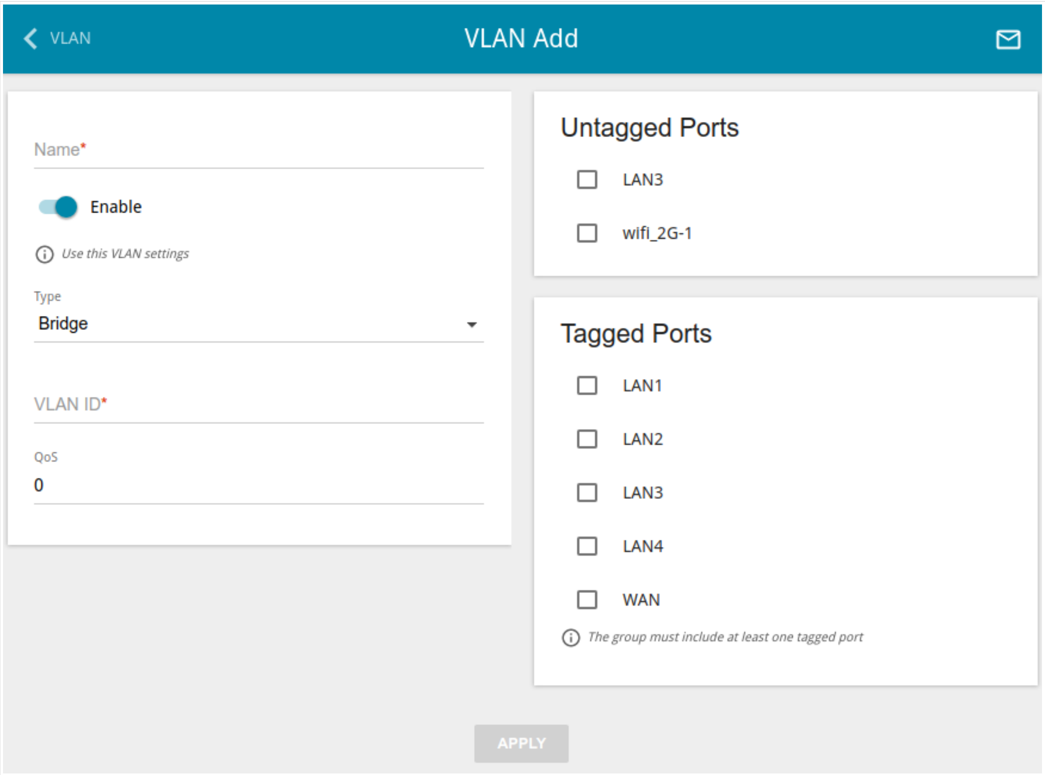
ADD DELETE

□	Name	Type	Untagged ports	Tagged port	VLAN ID	Enable
□	lan	Untagged LAN	LAN1, LAN2, LAN3, LAN4, wifi_2G-1, wifi_5G-1	-	-	Yes
□	wan	Untagged NAT	WAN	-	-	Yes

*Figure 127. The **Advanced / VLAN** page.*

If you want to create a group including LAN ports of the router, first delete relevant records from the **lan** group on this page. To do this, select the **lan** group. On the opened page, in the **Untagged Ports** section, deselect the checkbox located to the left of the relevant port, and click the **APPLY** button.

To create a new group for VLAN, click the **ADD** button.



Name*

Enable

Use this VLAN settings

Type
Bridge

VLAN ID*

QoS
0

Untagged Ports

□ LAN3
□ wifi_2G-1

Tagged Ports

□ LAN1
□ LAN2
□ LAN3
□ LAN4
□ WAN

The group must include at least one tagged port

Figure 128. The page for adding a group of ports for VLAN.

You can specify the following parameters:

Parameter	Description
Name	A name for the port for easier identification.
Enable	Move the switch to the right to allow using this group of ports.
Type	The type of the VLAN. **Untagged NAT**. The group of this type is an external connection with address translation. It is mostly used to transmit untagged traffic. When this value is selected, the **VLAN ID** and **QoS** fields and the **Tagged Ports** section are not displayed. Only one group of this type can exist in the system. **Tagged NAT**. The group of this type is an external connection with address translation. It is mostly used to connect to the Internet. Later the VLAN which identifier is specified in the **VLAN ID** field is used to create a WAN connection (on the **Connections Setup / WAN** page). When this value is selected, the **Untagged Ports** section is not displayed. **Bridge**. The group of this type is a transparent connection between an internal port and an external connection. It is mostly used to connect IPTV set-top boxes.
VLAN ID	An identifier of the VLAN to which this group of ports will be assigned.
QoS	A priority tag for the transmitted traffic.
Untagged Ports	The section includes the ports that can be added to the group. To add a port to the group, select the checkbox located to the left of the relevant port. To remove a port from the group, deselect the checkbox located to the left of the relevant port.
Tagged Ports	Select an available value to assign it to this group. To do this, select the checkbox located to the left of the relevant port.

Click the **APPLY** button.

To edit an existing group, select the relevant group in the table. On the page displayed, change the parameters and click the **APPLY** button.

To remove an existing group, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button.

DNS

On the **Advanced / DNS** page, you can add DNS servers to the system.

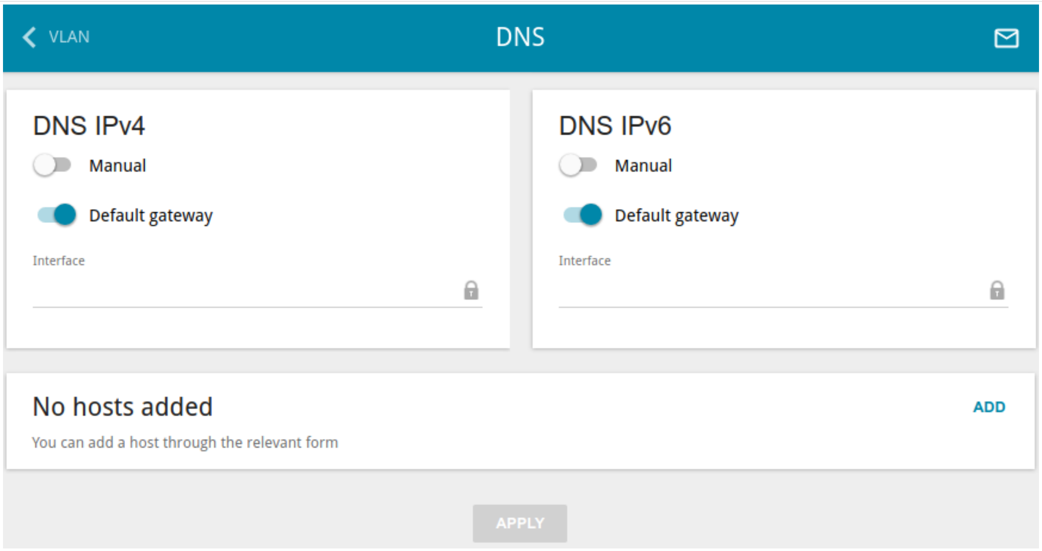


*Figure 129. The **Advanced / DNS** page.*

DNS servers are used to determine the IP address from the name of a server in Intranets or the Internet (as a rule, they are specified by an ISP or assigned by a network administrator).

You can specify the addresses of DNS servers manually on this page or configure the router to obtain DNS servers addresses automatically from your ISP upon installing a connection.

! When you use the built-in DHCP server, the network parameters (including DNS servers) are distributed to clients automatically.

If you want to configure automatic obtainment of DNS servers addresses, move the **Manual** switch to the left (use the **DNS IPv4** section for IPv4 and the **DNS IPv6** section for IPv6). Then move the **Default gateway** switch to the left and from the **Interface** drop-down list select a WAN connection which will be used to obtain addresses of DNS servers automatically. If you want the router to use the default WAN connection to obtain addresses of DNS servers, move the **Default gateway** switch to the right. Then click the **APPLY** button.

To specify a DNS server manually, move the **Manual** switch to the right (use the **DNS IPv4** section for IPv4 and the **DNS IPv6** section for IPv6). In the **Name Servers IPv4** or **Name Servers IPv6** section, click the **ADD SERVER** button, and in the line displayed, enter an IP address of the DNS server. Then click the **APPLY** button.

To remove a DNS server from the page, click the **Delete** icon (×) in the line of the address and then click the **APPLY** button.

If needed, you can add your own address resource record. To do this, click the **ADD** button.

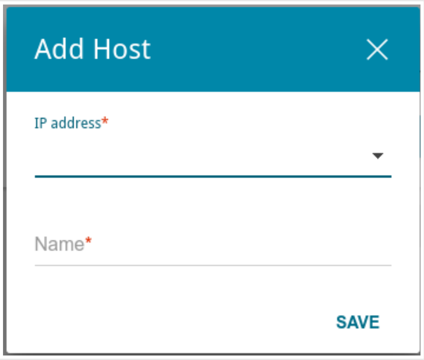


Figure 130. The window for adding a DNS record.

In the **IP address** field, specify a host from the internal or external network. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IP address from the drop-down list (the field will be filled in automatically). In the **Name** field, specify the domain name to which the specified IP address will correspond. Click the **SAVE** button.

To edit an existing record, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a record, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button.

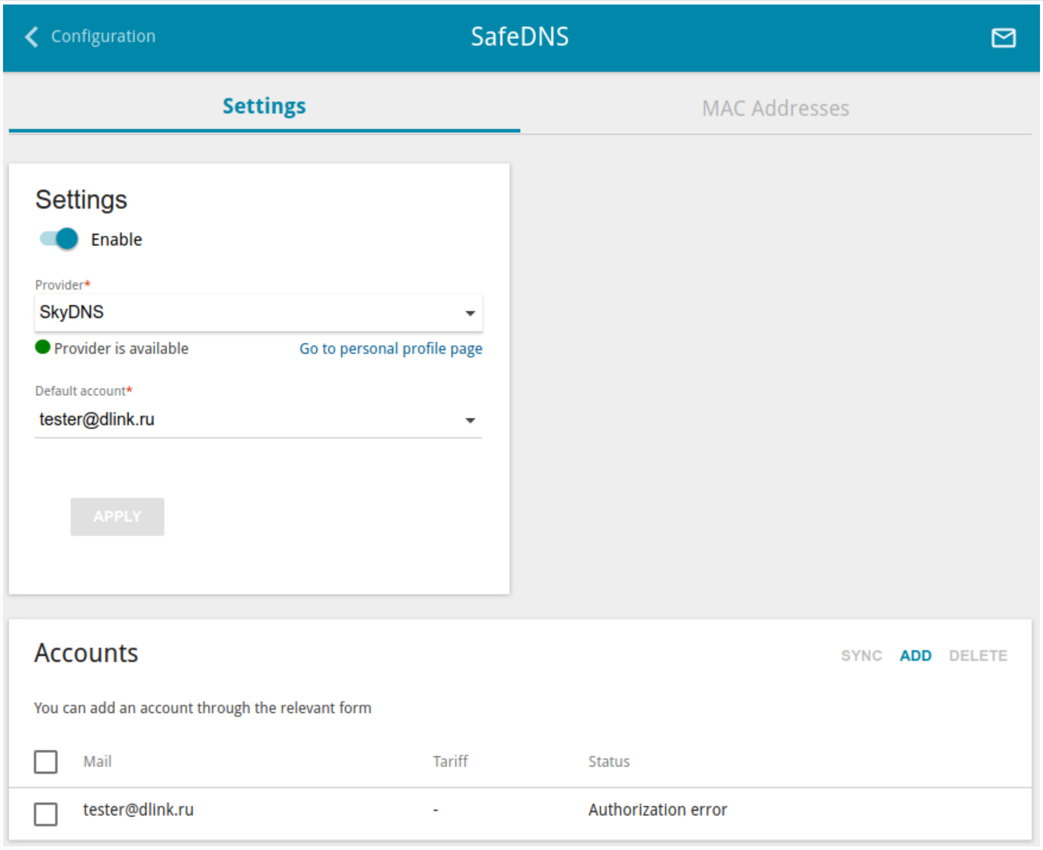
After completing the work with records, click the **APPLY** button.

SafeDNS

This page is designed to configure the SafeDNS/SkyDNS service.

SafeDNS and SkyDNS are web content filtering services which provide protection against malicious web sites for devices connected to the router's network, and also allow to configure filtering, block access to adult web sites, and use search engines safely. In order to use the service, first register an account on its provider's web site.

To enable the SafeDNS/SkyDNS service, on the **Settings** tab, move the **Enable** switch to the right.



Settings

Enable

Provider*: SkyDNS

● Provider is available

Go to personal profile page

Default account*: tester@dlink.ru

Accounts

You can add an account through the relevant form

□	Mail	Tariff	Status
□	tester@dlink.ru	-	Authorization error

*Figure 131. The **SafeDNS** page. The **Settings** tab.*

Select the needed value from the **Provider** drop-down list:

- **SkyDNS:** for the account registered on www.skydns.ru.
- **SafeDNS:** for the account registered on www.safedns.com.

Click the **APPLY** button.

Then click the **ADD** button to add an account which will be used for the service work.

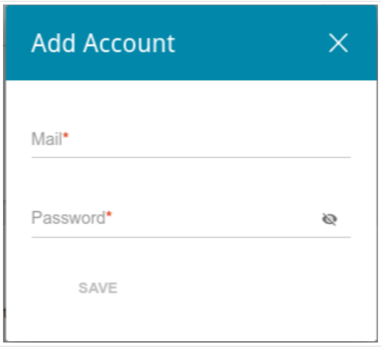


*Figure 132. The **SafeDNS** page. The window for adding an account.*

In the opened window, in the **Mail** and **Password** fields, enter the account data (the e-mail address and the password correspondingly) specified upon registration on the web site of the provider. Then click the **SAVE** button.

Select your account from the **Default account** drop-down list. Then from the **Default profile** list displayed, select the filtering profile which will be used for all devices of your LAN. Click the **APPLY** button.

The default filtering profile will be applied to all devices newly connected to the router's network.

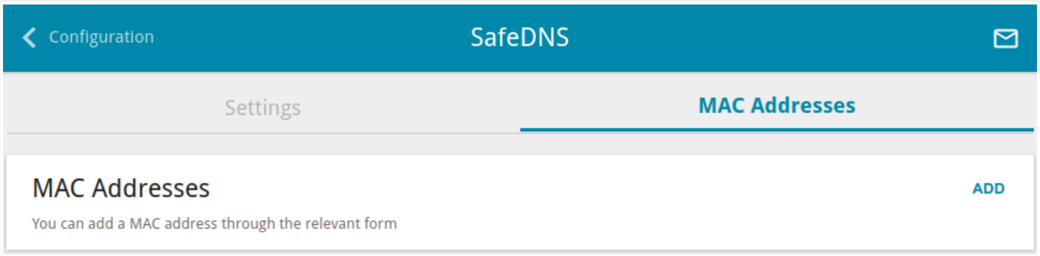
To change the parameters of your account on the web site of the provider, click the **Go to personal profile page** link.

By default, the account parameters are automatically synchronized with the provider's web site once an hour. To start synchronization manually, in the **Accounts** section, select the checkbox located to the left of the relevant line in the table and click the **SYNC** button.

To change the password of the account, in the **Accounts** section, select the relevant line in the table. In the opened window, change the password and click the **SAVE** button.

To remove the account, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button.

If it is necessary to assign a specific filtering profile to a device connected to the router's network, go to the **MAC Addresses** tab.



MAC Addresses

You can add a MAC address through the relevant form

*Figure 133. The **SafeDNS** page. The **MAC Addresses** tab.*

Click the **ADD** button.

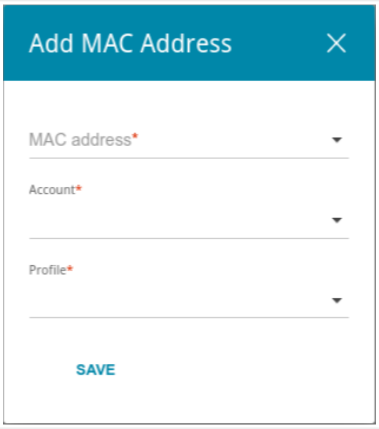


*Figure 134. The **SafeDNS** page. The window for adding a rule.*

In the window displayed, specify the following parameters:

Parameter	Description
MAC address	The MAC address of a device from the router's LAN to which the specified filtering profile will be applied. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
Account	Select your account from the drop-down list.
Profile	Select the filtering profile which will be used for the device with the specified MAC address from the drop-down list.

Click the **SAVE** button.

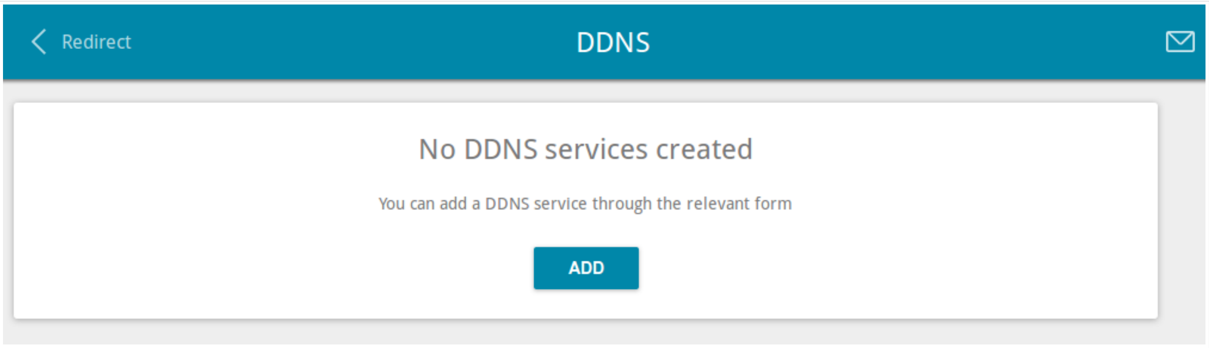
To edit a rule, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a rule, select the checkbox located to the left of the relevant line of the table and click the **DELETE** button.

To disable the SafeDNS/SkyDNS service, move the **Enable** switch to the left and click the **APPLY** button.

DDNS

On the **Advanced / DDNS** page, you can define parameters of the DDNS service, which allows associating a domain name with dynamic IP addresses.

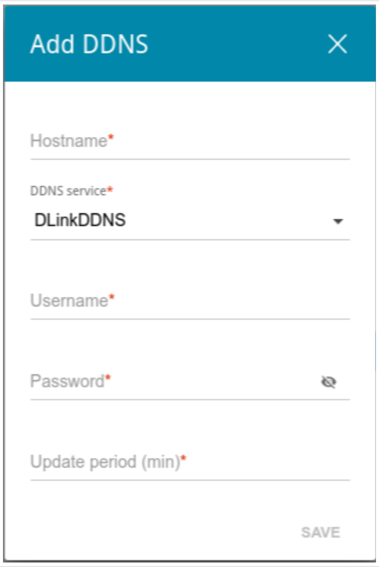


No DDNS services created

You can add a DDNS service through the relevant form

*Figure 135. The **Advanced / DDNS** page.*

To add a new DDNS service, click the **ADD** button.


Add DDNS

Hostname*

DDNS service*: DLinkDDNS

Username*

Password*

Update period (min)*

Figure 136. The window for adding a DDNS service.

In the opened window, you can specify the following parameters:

Parameter	Description
Hostname	The full domain name registered at your DDNS provider.
DDNS service	Select a DDNS provider from the drop-down list.
Username	The username to authorize for your DDNS provider.
Password	The password to authorize for your DDNS provider. Click the **Show** icon (👁) to display the entered password.
Update period	An interval (in minutes) between sending data on the router's external IP address to the relevant DDNS service.

After specifying the needed parameters, click the **SAVE** button.

To edit parameters of the existing DDNS service, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove an existing DDNS service, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button.

Redirect

On the **Advanced / Redirect** page, you can enable notifications on the reason of the Internet connection failure. Notifications will be displayed in the browser window when a user is attempting to open a web site on the Internet.

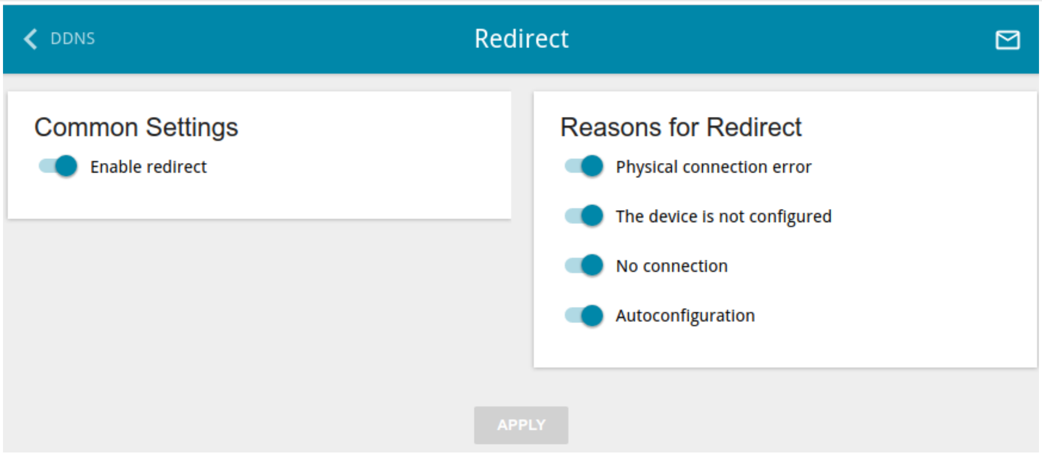


*Figure 137. The **Advanced / Redirect** page.*

To configure notifications, in the **Common Settings** section, move the **Enable redirect** switch to the right. Then, in the **Reasons for Redirect** section, move the needed switches to the right.

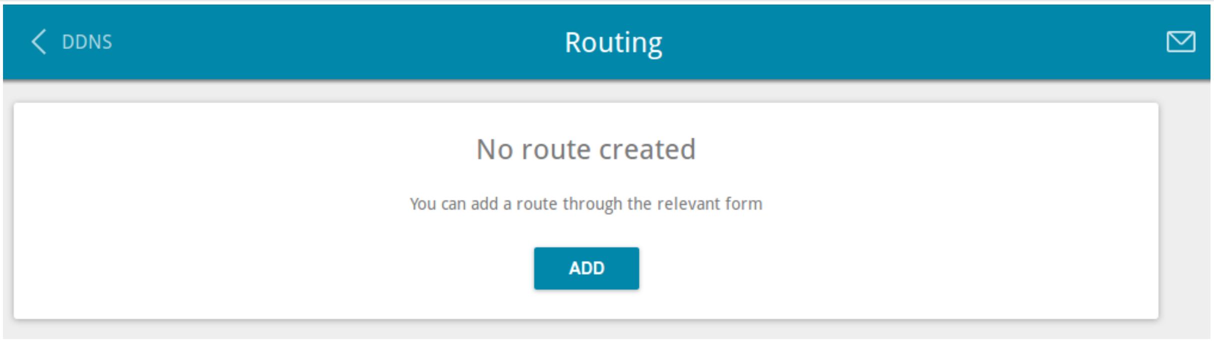
Parameter	Description
Reasons for Redirect	
Physical connection error	Notifications in case of physical connection problems (the ISP's cable is not connected, an additional device needed to access the Internet is not connected).
The device is not configured	Notifications in case when the device works with default settings.
No connection	Notifications in case of problems of the default WAN connection (authorization error, the IPS's server does not respond, etc.).
Autoconfiguration	Notifications in case when the ISP's auto configuration server is configuring the device remotely.

When you have configured the parameters, click the **APPLY** button.

To disable notifications, move the **Enable redirect** switch to the left and click the **APPLY** button.

Routing

On the **Advanced / Routing** page, you can add static routes (routes for networks that are not connected directly to the device but are available through the interfaces of the device) into the system.

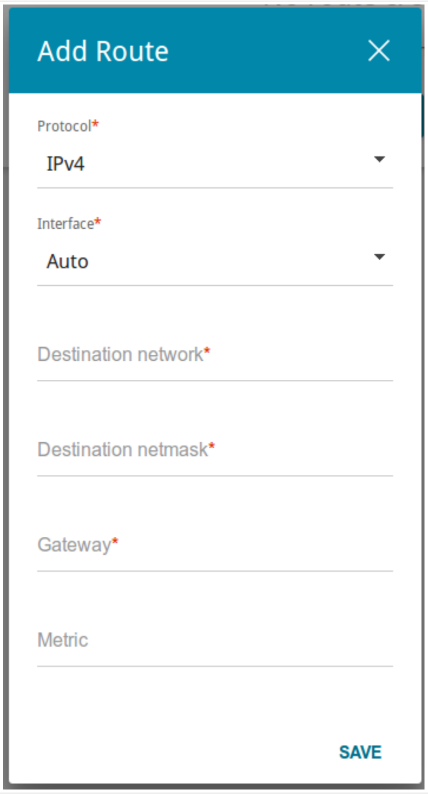


No route created

You can add a route through the relevant form

*Figure 138. The **Advanced / Routing** page.*

To create a new route, click the **ADD** button.



Protocol*: IPv4

Interface*: Auto

Destination network*

Destination netmask*

Gateway*

Metric

Figure 139. The window for adding a new route.

In the opened window, you can specify the following parameters:

Parameter	Description
Protocol	A protocol that the route will use.
Interface	From the drop-down list, select an interface through which the destination network can be accessed. If you have selected the **Auto** value, the router itself sets the interface on the basis of data on connected networks.
Destination network	A destination network to which this route is assigned. You can specify an IPv4 or IPv6 address. You can specify an IPv6 address (`2001:db8:1234::1`) or an IPv6 address with a prefix (`2001:db8:1234::/64`).
Destination netmask	*For IPv4 protocol only.* The destination network mask.
Gateway	An IP address through which the destination network can be accessed.
Metric	A metric for the route. The lower the value, the higher is the route priority. *Optional*.

After specifying the needed parameters, click the **SAVE** button.

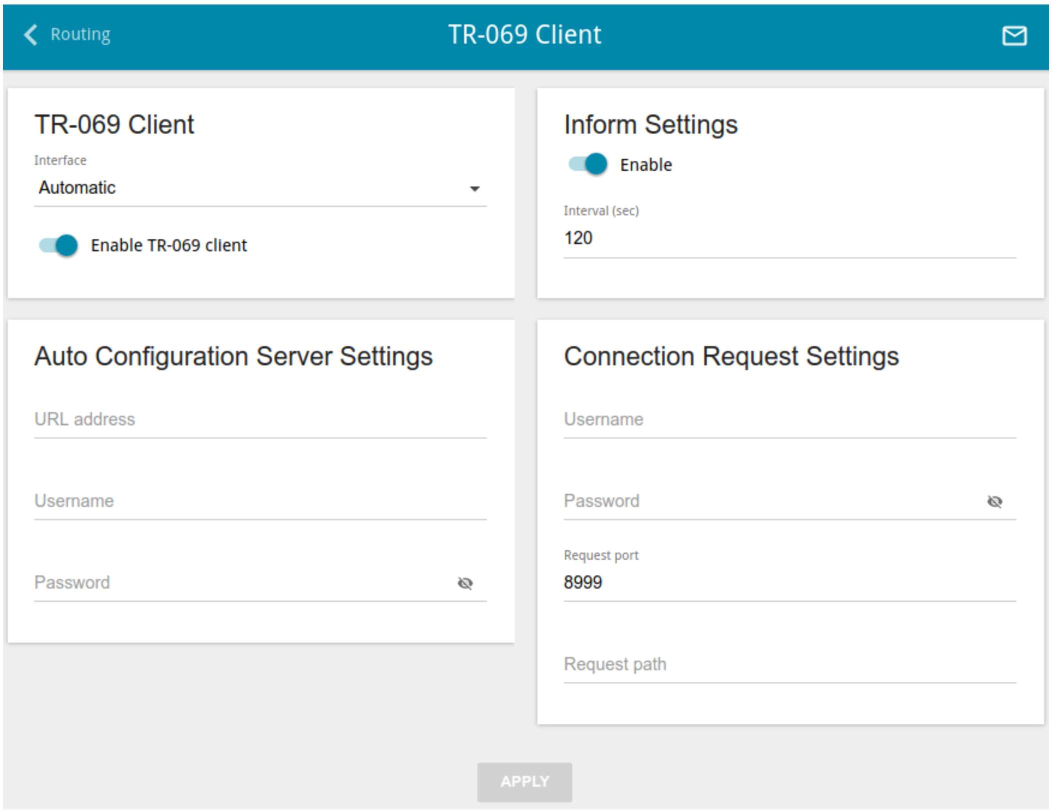
To edit an existing route, select a relevant line of the table. On the opened page, change the needed parameters and click the **SAVE** button.

To remove an existing route, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button.

TR-069 Client

On the **Advanced / TR-069 Client** page, you can configure the router for communication with a remote Auto Configuration Server (ACS).

The TR-069 client is used for remote monitoring and management of the device.



TR-069 Client
Interface: Automatic
Enable TR-069 client

Inform Settings
Enable
Interval (sec): 120

Auto Configuration Server Settings
URL address
Username
Password

Connection Request Settings
Username
Password
Request port: 8999
Request path

Figure 140. The page for configuring the TR-069 client.

You can specify the following parameters:

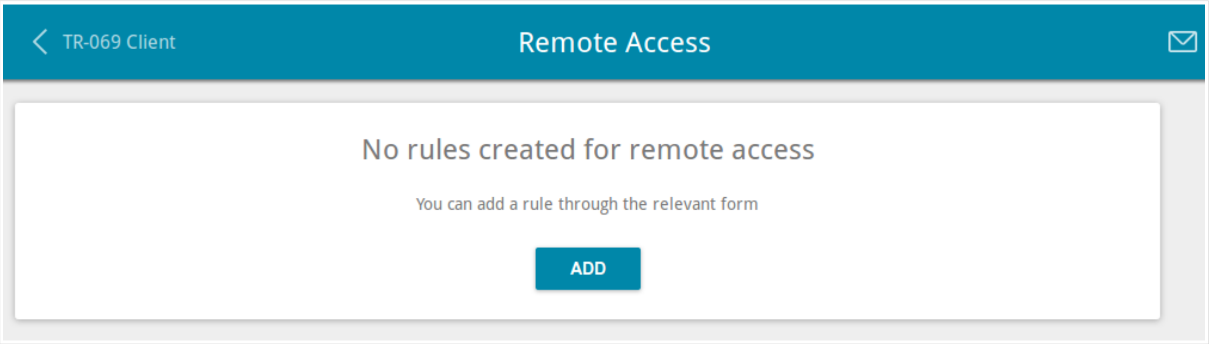
Parameter	Description
TR-069 Client	
Interface	The interface which the router uses for communication with the ACS. Leave the **Automatic** value to let the device select the interface basing on the routing table or select another value if required by your ISP.
Enable TR-069 client	Move the switch to the right to enable the TR-069 client.
Inform Settings	
Enable	Move the switch to the right so the router may send reports (data on the device and network statistics) to the ACS.
Interval	Specify the time period (in seconds) between sending reports.

Parameter	Description
Auto Configuration Server Settings	
URL address	The URL address of the ACS provided by the ISP.
Username	The username to connect to the ACS.
Password	The password to connect to the ACS.
Connection Request Settings	
Username	The username used by the ACS to transfer a connection request to the router.
Password	The password used by the ACS.
Request port	The port used by the ACS. By default, the port `8999` is specified.
Request path	The path used by the ACS.

When you have configured the parameters, click the **APPLY** button.

Remote Access

On the **Advanced / Remote Access** page, you can configure access to the web-based interface of the router. By default, the access from external networks to the router is closed. If you need to allow access to the router from the external network, create relevant rules.

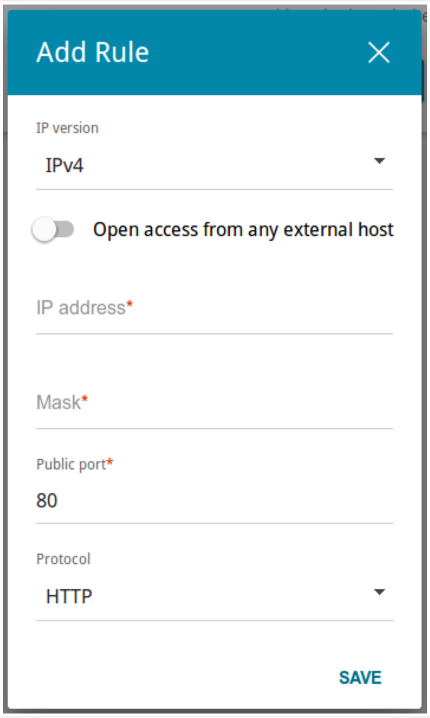


No rules created for remote access

You can add a rule through the relevant form

*Figure 141. The **Advanced / Remote Access** page.*

To create a new rule, click the **ADD** button.



IP version: IPv4

Open access from any external host

IP address*

Mask*

Public port*: 80

Protocol: HTTP

Figure 142. The window for adding a rule for remote management.

In the opened window, you can specify the following parameters:

Parameter	Description
IP version	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
Open access from any external host	Move the switch to the right to allow access to the router for any host. Upon that the **IP address** and **Mask** fields are not displayed.

Parameter	Description
IP address	A host or a subnet to which the rule is applied. You can specify an IPv4 or IPv6 address.
Mask	*For the IPv4-based network only.* The mask of the subnet.
Public port	*For the IPv4-based network only.* An external port of the router. You can specify only one port.
Protocol	The protocol available for remote management of the router.

After specifying the needed parameters, click the **SAVE** button.

To edit a rule for remote access, left-click the relevant rule. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a rule for remote access, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button.

UPnP IGD

On the **Advanced / UPnP IGD** page, you can enable the UPnP IGD protocol. The router uses the UPnP IGD protocol for automatic configuration of its parameters for network applications requiring an incoming connection to the router.

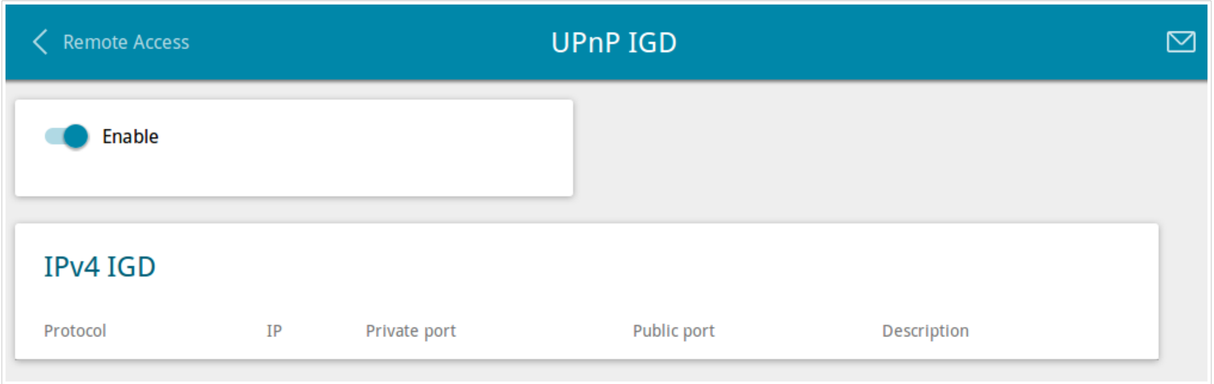


*Figure 143. The **Advanced / UPnP IGD** page.*

If you want to manually specify all parameters needed for network applications, move the **Enable** switch to the left. Then go to the **Firewall / Virtual Servers** page and specify needed settings.

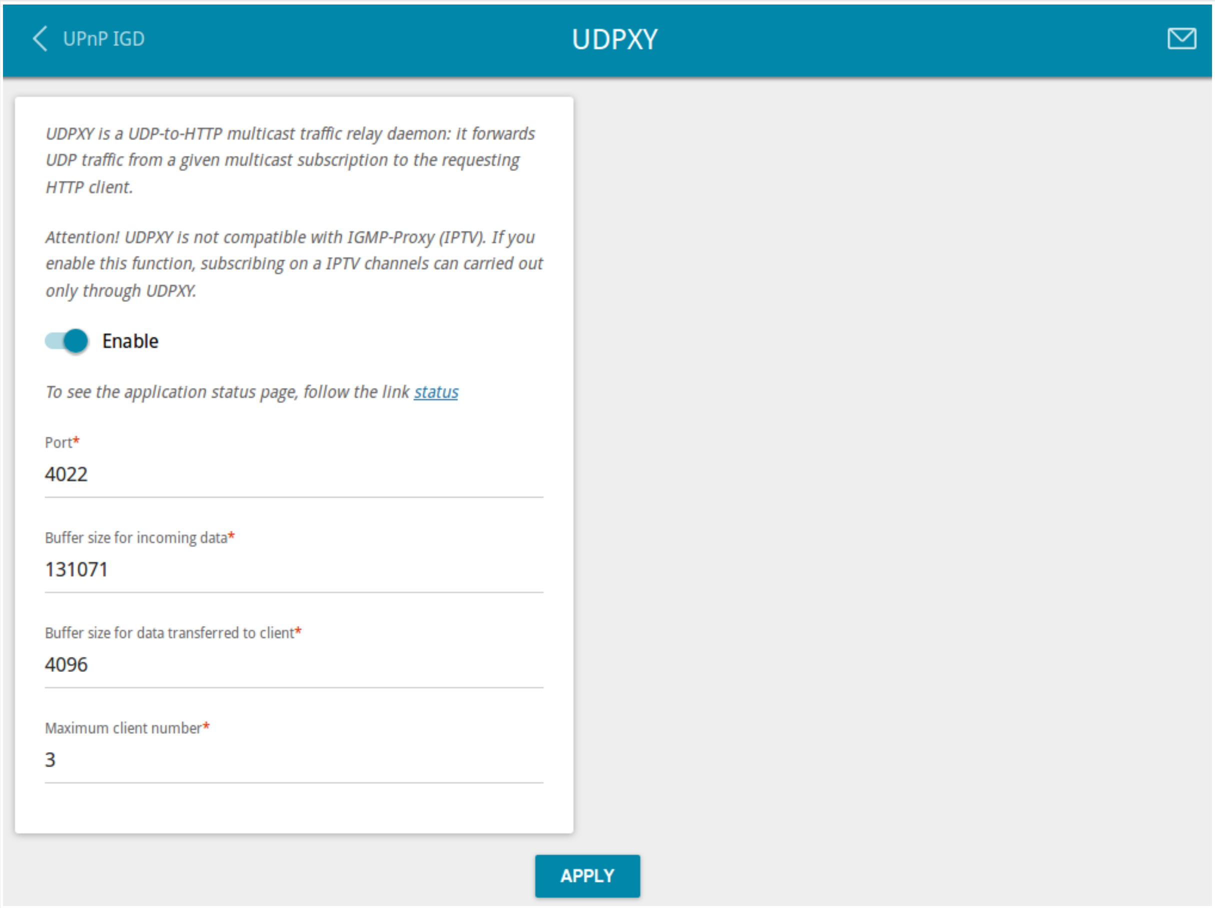
If you want to enable the UPnP IGD protocol in the router, move the **Enable** switch to the right.

When the protocol is enabled, the router's parameters configured automatically are displayed on the page:

Parameter	Description
Protocol	A protocol for network packet transmission.
IP	The IP address of a client from the local area network.
Private port	A port of a client's IP address to which traffic is directed from a public port of the router.
Public port	A public port of the router from which traffic is directed to a client's IP address.
Description	Information transmitted by a client's network application.

UDPXY

On the **Advanced / UDPXY** page, you can allow the router to use the built-in UDPXY application. The UDPXY application transforms UDP traffic into HTTP traffic. This application allows devices which cannot receive UDP streams to access stream video.



UDPXY is a UDP-to-HTTP multicast traffic relay daemon: it forwards UDP traffic from a given multicast subscription to the requesting HTTP client.

Attention! UDPXY is not compatible with IGMP-Proxy (IPTV). If you enable this function, subscribing on a IPTV channels can carried out only through UDPXY.

● Enable

To see the application status page, follow the link status

Port*
4022

Buffer size for incoming data*
131071

Buffer size for data transferred to client*
4096

Maximum client number*
3

*Figure 144. The **Advanced / UDPXY** page.*

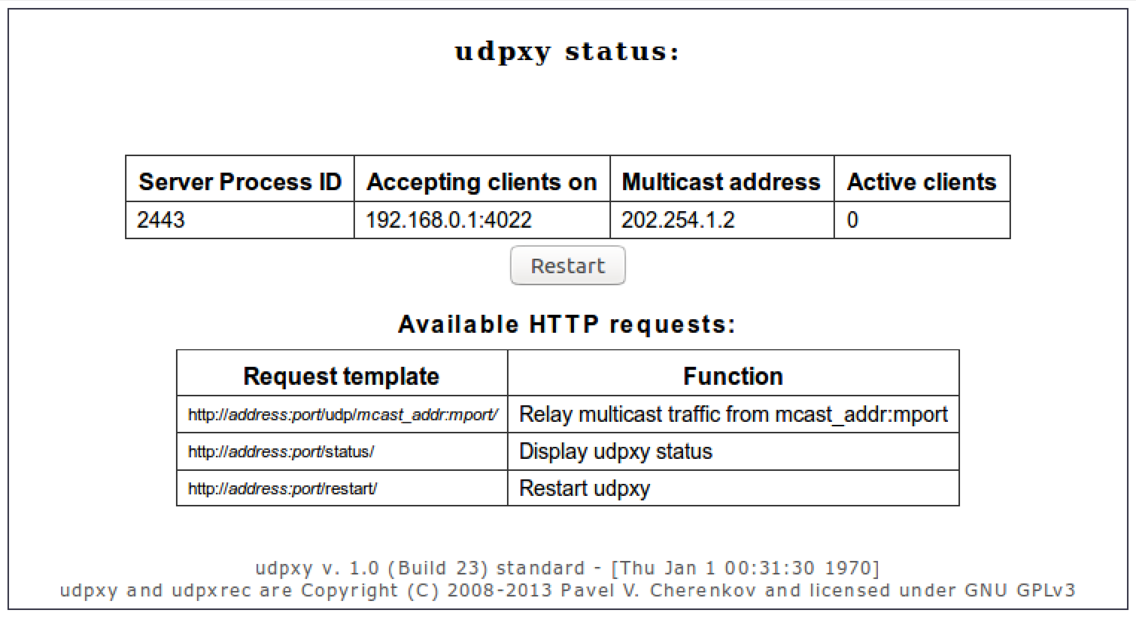
To enable the application, move the **Enable** switch to the right. When the application is enabled, the IGMP Proxy function is automatically disabled.

Upon that the following fields are displayed on the page:

Parameter	Description
Port	The port of the router which the UDPXY application uses.
Buffer size for incoming data	Size of intermediate buffer for received data. By default, the minimum acceptable value is specified.
Buffer size for data transferred to client	Size of intermediate buffer for transmitted data. By default, the minimum acceptable value is specified.
Maximum client number	Maximum number of devices from the router's LAN which will be served by the application.

After specifying the needed parameters, click the **APPLY** button.

To access the status page of the application, click the **status** link.



udpxy status:

Server Process ID	Accepting clients on	Multicast address	Active clients
2443	192.168.0.1:4022	202.254.1.2	0

Available HTTP requests:

Request template	Function
http://*address*:*port*/udp/*mcast_addr*:*mport*/	Relay multicast traffic from mcast_addr:mport
http://*address*:*port*/status/	Display udpxy status
http://*address*:*port*/restart/	Restart udpxy

udpxy v. 1.0 (Build 23) standard - [Thu Jan 1 00:31:30 1970]
udpxy and udpxrec are Copyright (C) 2008-2013 Pavel V. Cherenkov and licensed under GNU GPLv3

Figure 145. The UDPXY application status page.

IGMP/ALG/Passthrough

On the **Advanced / IGMP/ALG/Passthrough** page, you can allow the router to use IGMP and RTSP, enable the SIP ALG and PPPoE/PPTP/L2TP/IPsec pass through functions.

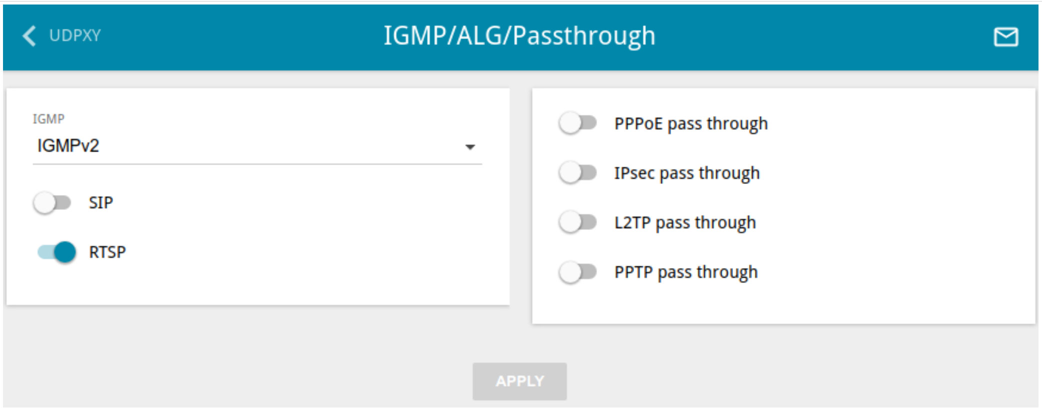
IGMP is used for managing multicast traffic (transferring data to a group of destinations). This protocol allows using network resources for some applications, e.g., for streaming video, more efficiently.

SIP is used for creating, modifying, and terminating communication sessions. This protocol allows telephone calls via the Internet.

RTSP is used for real-time streaming multimedia data delivery. This protocol allows some applications to receive streaming audio/video from the Internet.

The PPPoE pass through function allows PPPoE clients of computers from your LAN to connect to the Internet through connections of the router.

The PPTP pass through, L2TP pass through and IPsec pass through functions allow VPN PPTP, L2TP and IPsec traffic to pass through the router so that clients from your LAN can establish relevant connections with remote networks.



IGMP: IGMPv2

SIP ○

RTSP ●

PPPoE pass through ○

IPsec pass through ○

L2TP pass through ○

PPTP pass through ○

*Figure 146. The **Advanced / IGMP/ALG/Passthrough** page.*

The following elements are available on the page:

Parameter	Description
IGMP	Select a version of IGMP from the drop-down list. Such a setting allows to enable multicasting from the WAN connection selected in the **IGMP** section on the **Connections Setup / WAN** page.
SIP	Move the switch to the right to enable SIP. Such a setting allows using the SIP ALG function. This function allows VoIP traffic to pass through the NAT-enabled router.[15]
RTSP	Move the switch to the right to enable RTSP. Such a setting allows managing media stream: fast forward streaming audio/video, pause and start it.
PPPoE pass through	Move the switch to the right to enable the PPPoE pass through function.
IPsec pass through	Move the switch to the right to enable the IPsec pass through function.
L2TP pass through	Move the switch to the right to enable the L2TP pass through function.
PPTP pass through	Move the switch to the right to enable the PPTP pass through function.

After specifying the needed parameters, click the **APPLY** button.

[15] On the **Connections Setup / WAN** page, create a WAN connection, move the **SIP** switch to the right on the **Advanced / IGMP/ALG/Passthrough** page, connect an Ethernet cable between a LAN port of the router and the IP phone. Specify SIP parameters on the IP phone and configure it to obtain an IP address automatically (as DHCP client).

IPsec

On the **Advanced / IPsec** page, you can configure VPN tunnels based on IPsec protocol.

IPsec is a protocol suite for securing IP communications.

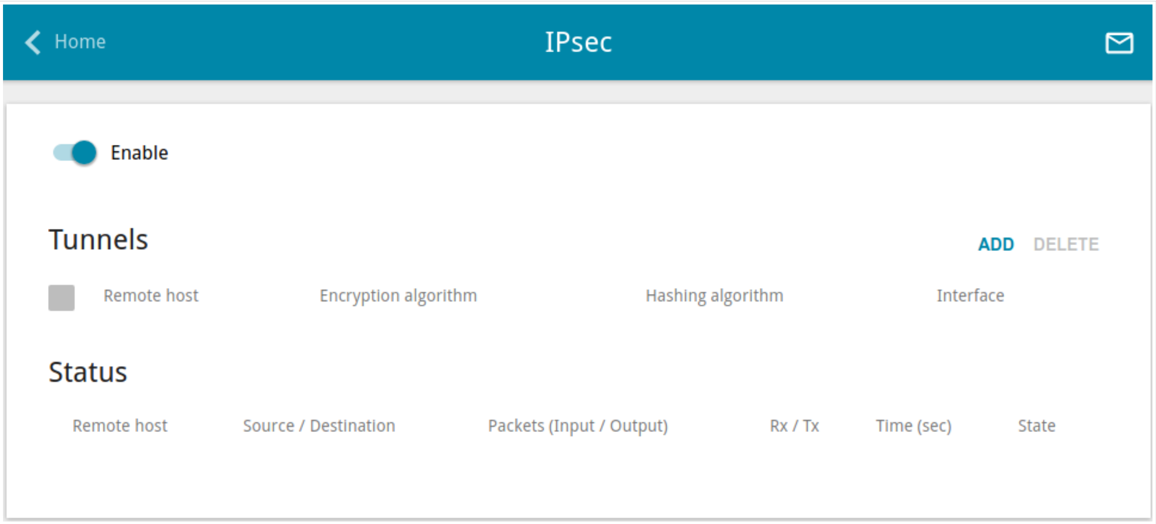


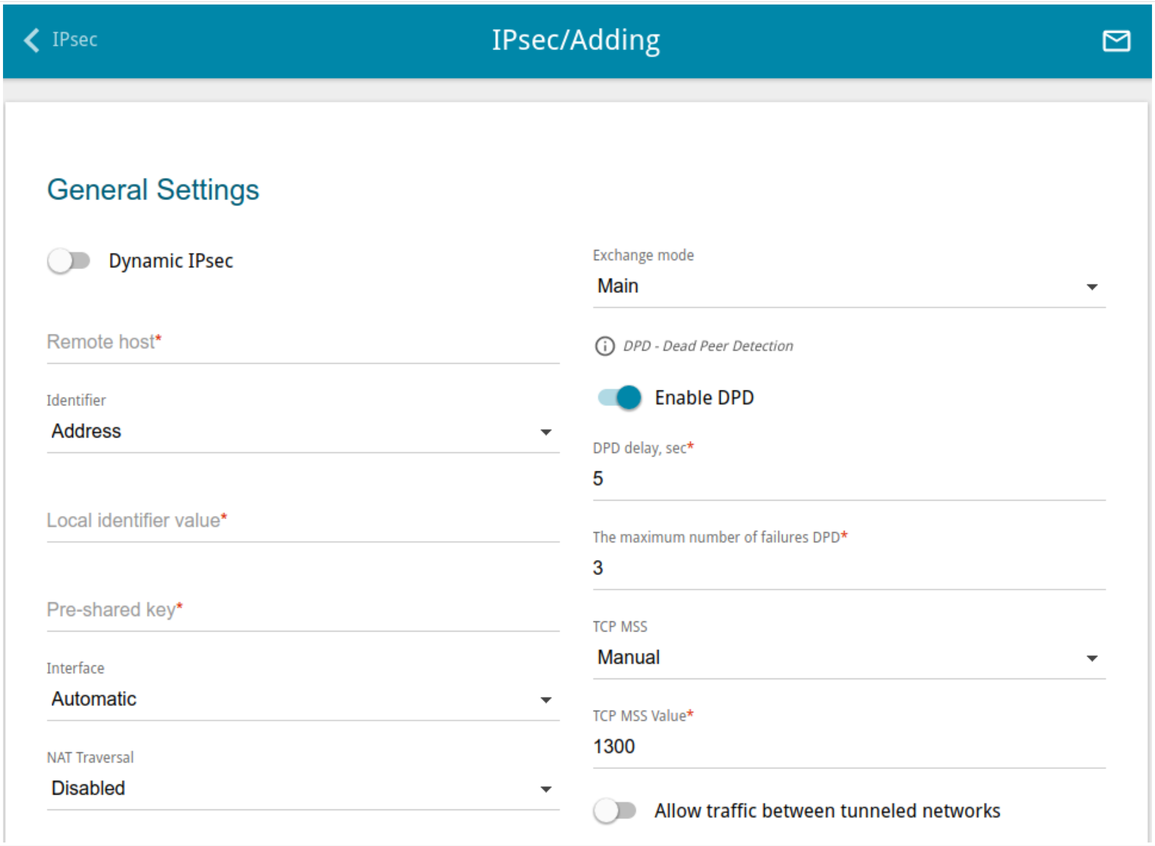
*Figure 147. The **Advanced / IPsec** page.*

To allow IPsec tunnels, move the **Enable** switch to the right. Upon that the **Tunnels** and **Status** sections are displayed on the page.

In the **Status** section, the current state of an existing tunnel is displayed.

To create a new tunnel, click the **ADD** button in the **Tunnels** section.

! Setting for both devices which establish the tunnel should be the same.



IPsec

IPsec/Adding

General Settings

Dynamic IPsec

Remote host*

Identifier: Address

Local identifier value*

Pre-shared key*

Interface: Automatic

NAT Traversal: Disabled

Exchange mode: Main

DPD - Dead Peer Detection

Enable DPD

DPD delay, sec*: 5

The maximum number of failures DPD*: 3

TCP MSS: Manual

TCP MSS Value*: 1300

Allow traffic between tunneled networks

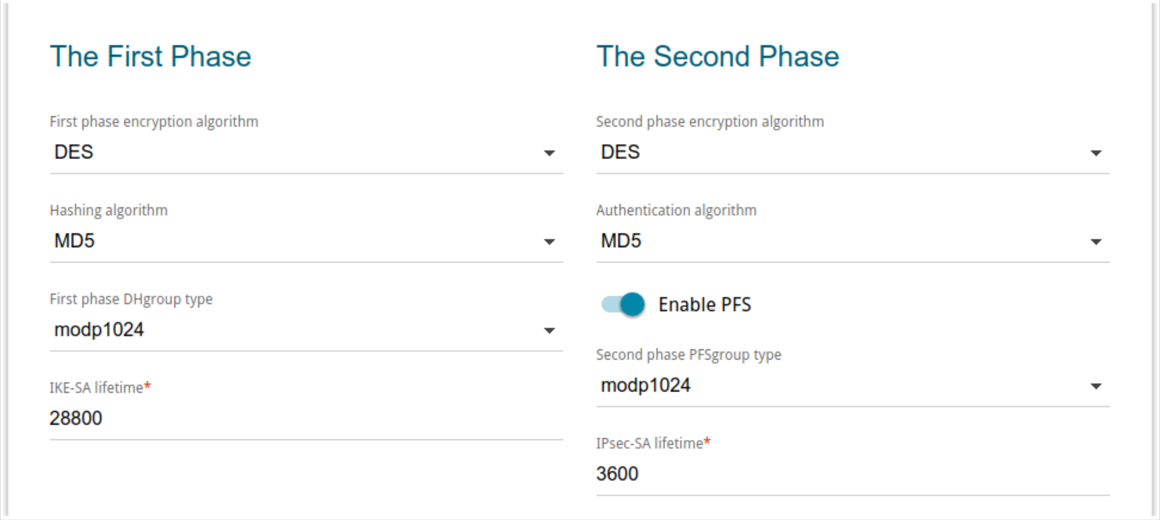
*Figure 148. The page for adding an IPsec tunnel. The **General Settings** section.*

You can specify the following parameters:

Parameter	Description
General Settings	
Dynamic IPsec	Move the switch to the right to allow a remote host with any public IP address to connect to the router via IPsec protocol. Such a setting can be specified for one tunnel only. Connection requests via this tunnel can be sent by a remote host only.
Remote host	A remote subnet VPN gateway IP address. The field is available, if the **Dynamic IPsec** switch is moved to the left.

Parameter	Description
Identifier	Select an identification method for the local host (router) from the drop-down list: **Address:** The local host is identified by its IP address. **FQDN:** The local host is identified by its domain name. The value is unavailable, if the **Main** value is selected from the **Exchange mode** list.
Local identifier value	Specify the local host identifier.
Pre-shared key	A key for mutual authentication of the parties.
Interface	Select a WAN connection through which the tunnel will pass. When the **Automatic** value is selected, the router uses the default WAN connection.
NAT Traversal	The NAT Traversal function allows VPN traffic to pass through the NAT-enabled router. Select the **Disabled** value to disable the function**.** Select the **Enabled** value to enable the function if it is supported by a remote host. Select the **Force** value to make the function be always on, even if it is not supported by a remote host.
Exchange mode	Select the mode of negotiation from the drop-down list: **Main:** The mode provides the most secure communication between the parties in the course of negotiation of the authentication procedures. **Base:** The draft negotiation mode with preliminary authentication of a host. **Aggressive:** The mode provides faster operation as it skips several stages of negotiation of the authentication procedures.
Enable DPD	Move the switch to the right to enable using DPD protocol for this tunnel. Such a setting allows to check the status of a remote host: if encrypted packets exchange between the router and the remote host breaks down, the router starts sending DPD messages to the remote host. If the switch is moved to to the left, the **DPD delay** and **The maximum number of failures DPD** fields are not available for editing.
DPD delay	A time period (in seconds) between attempts to check the status of a remote host. By default, the value **5** is specified.

Parameter	Description
The maximum number of failures DPD	A number of DPD messages that were sent to check the status of a remote host and left unanswered. By default, the value **3** is specified. If a remote host does not answer the specified number of messages, the router breaks down the tunnel connection, removes the encryption keys, and tries to activate the connection.
TCP MSS	*Maximum Segment Size of a TCP packet.* This parameter influences the size of a TCP packet which will be sent from a remote host to the router. If the **Manual** value is selected, you can specify the parameter in the **TCP MSS Value** field. If the **Path MTU discovery** value is selected, the parameter will be configured automatically.
TCP MSS Value	The maximum size (in bytes) of a non-fragmented packet. The field is available for editing when the **Manual** value is selected from the **TCP MSS** drop-down list.
Allow traffic between tunneled networks	Move the switch to the right to allow data exchange between subnets with which IPsec tunnels have been created.



The First Phase

First phase encryption algorithm: DES

Hashing algorithm: MD5

First phase DHgroup type: modp1024

IKE-SA lifetime*: 28800

The Second Phase

Second phase encryption algorithm: DES

Authentication algorithm: MD5

Enable PFS

Second phase PFSgroup type: modp1024

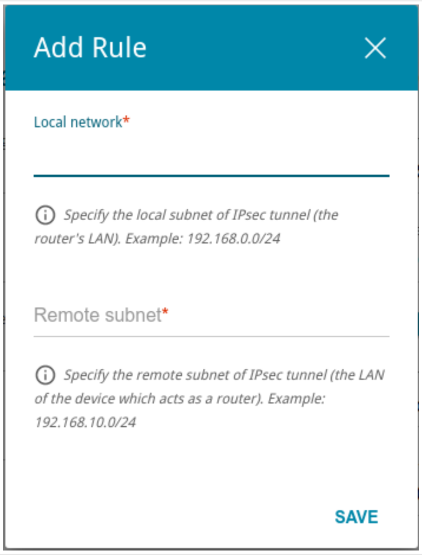
IPsec-SA lifetime*: 3600

*Figure 149. The page for adding an IPsec tunnel. **The First Phase / The Second Phase** sections.*

Parameter	Description
The First Phase	
First phase encryption algorithm	Select encryption algorithm from the drop-down list.
Hashing algorithm	Select hashing algorithm from the drop-down list.
First phase DHgroup type	A Diffie-Hellman key group for Phase 1. Select a value from the drop-down list.
IKE-SA lifetime	The lifetime of IKE-SA keys in seconds. After the specified period it is required to renegotiate the keys. The value specified in this field should exceed the value specified in the **IPsec-SA lifetime** field. Specify **0** if you don't want to limit the lifetime of the keys.
The Second Phase	
Second phase encryption algorithm	Select encryption algorithm from the drop-down list.
Authentication algorithm	Select authentication algorithm from the drop-down list.
Enable PFS	Move the switch to the right to enable the PFS option (*Perfect Forward Secrecy*). If the is moved to the right, a new encryption key exchange will be used for Phase 2. This option increases the security level of data transfer.
Second phase PFSgroup type	A Diffie-Hellman key group for Phase 2. Select a value from the drop-down list. The field is available, if the **Enable PFS** switch is moved to the right.

Parameter	Description
IPsec-SA lifetime	The lifetime of IPsec-SA keys in seconds. After the specified period it is required to renegotiate the keys. Specify 0 if you don't want to limit the lifetime of the keys.

If you need to specify IP addresses of local and remote subnets for creating a tunnel, click the **ADD** button in the **Tunneled Networks** section.



ⓘ Specify the local subnet of IPsec tunnel (the router's LAN). Example: 192.168.0.0/24

ⓘ Specify the remote subnet of IPsec tunnel (the LAN of the device which acts as a router). Example: 192.168.10.0/24

Figure 150. The page for adding an IPsec tunnel. The window for adding a tunneled network.

In the opened window, you can specify the following parameters:

Parameter	Description
Local network	A local subnet IP address and mask.
Remote subnet	A remote subnet IP address and mask.

To edit fields in the **Tunneled Networks** section, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a subnet, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button. Also you can remove a subnet in the editing window.

After configuring all needed settings for the IPsec tunnel, click the **APPLY** button.

To edit the parameters of an existing tunnel, in the **Tunnels** section, select the relevant tunnel in the table. On the opened page, change the needed parameters and click the **APPLY** button.

To remove an existing tunnel, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button. Also you can remove a tunnel on the editing page.

To disable VPN tunnels based on IPsec protocol, move the **Enable** switch to the left.

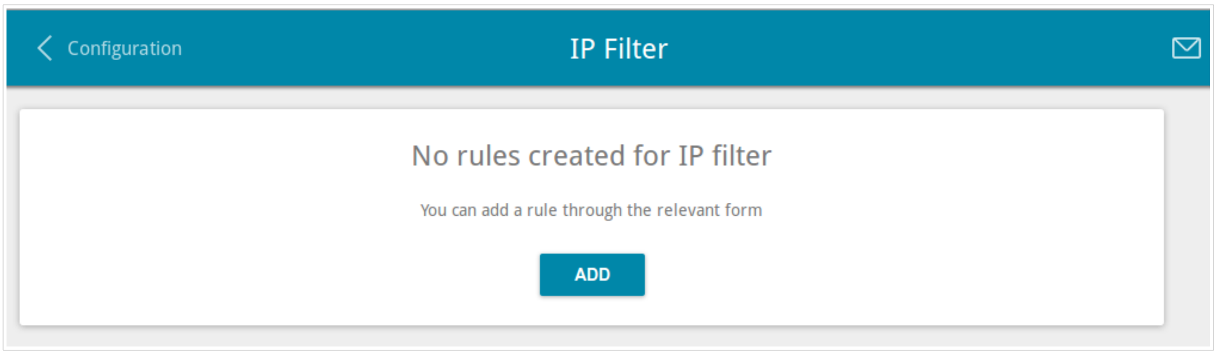
Firewall

In this menu you can configure the firewall of the router:

- add rules for IP filtering
- create virtual servers
- define a DMZ
- configure the MAC filter
- specify restrictions on access to certain web sites.

IP Filter

On the **Firewall / IP Filter** page, you can create new rules for filtering IP packets and edit or remove existing rules.

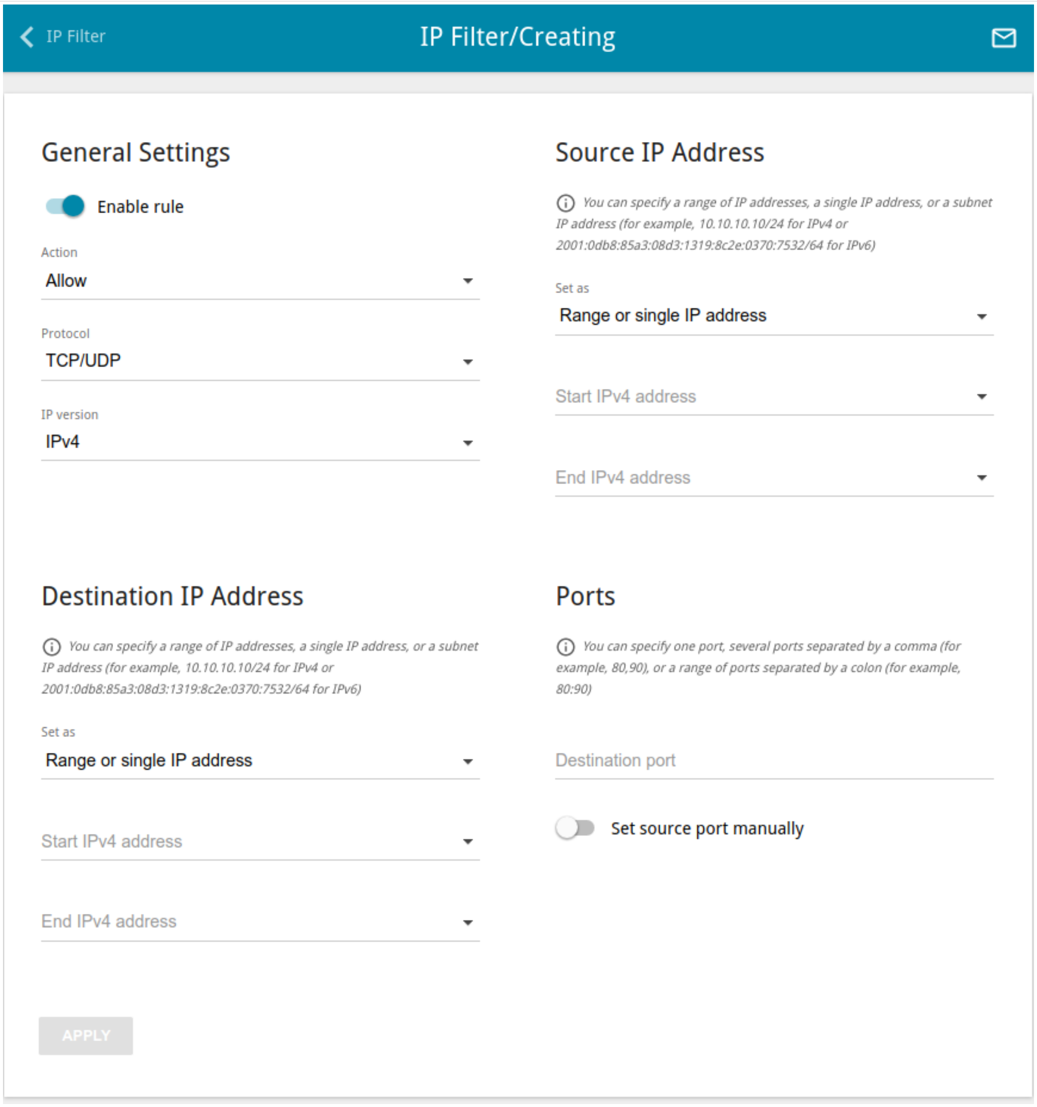


No rules created for IP filter

You can add a rule through the relevant form

*Figure 151. The **Firewall / IP Filter** page.*

To create a new rule, click the **ADD** button.



General Settings

Enable rule

Action
Allow

Protocol
TCP/UDP

IP version
IPv4

Source IP Address

You can specify a range of IP addresses, a single IP address, or a subnet IP address (for example, 10.10.10.10/24 for IPv4 or 2001:0db8:85a3:08d3:1319:8c2e:0370:7532/64 for IPv6)

Set as
Range or single IP address

Start IPv4 address

End IPv4 address

Destination IP Address

You can specify a range of IP addresses, a single IP address, or a subnet IP address (for example, 10.10.10.10/24 for IPv4 or 2001:0db8:85a3:08d3:1319:8c2e:0370:7532/64 for IPv6)

Set as
Range or single IP address

Start IPv4 address

End IPv4 address

Ports

You can specify one port, several ports separated by a comma (for example, 80,90), or a range of ports separated by a colon (for example, 80:90)

Destination port

Set source port manually

Figure 152. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description
General Settings	
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Action	Select an action for the rule. **Allow**: Allows packet transmission in accordance with the criteria specified by the rule. **Deny**: Denies packet transmission in accordance with the criteria specified by the rule.
Protocol	A protocol for network packet transmission. Select a value from the drop-down list.

Parameter	Description
IP version	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
Source IP Address	
Set as	Select the needed value from the drop-down list.
Start IPv4 address / Start IPv6 address	The source host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the **End IPv4 address / End IPv6 address** field blank. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).
End IPv4 address / End IPv6 address	The source host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The source subnet IPv4 or IPv6 address. The field is displayed when the **Subnet** value is selected from the **Set as** drop-down list.
Destination IP Address	
Set as	Select the needed value from the drop-down list.
Start IPv4 address / Start IPv6 address	The destination host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the **End IPv4 address / End IPv6 address** field blank. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).
End IPv4 address / End IPv6 address	The destination host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The destination subnet IPv4 or IPv6 address. The field is displayed when the **Subnet** value is selected from the **Set as** drop-down list.
Ports	
Destination port	A port of the destination IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.
Set source port manually	Move the switch to the right to specify a port of the source IP address manually. Upon that the **Source port** field is displayed.

Parameter	Description
Source port	A port of the source IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.

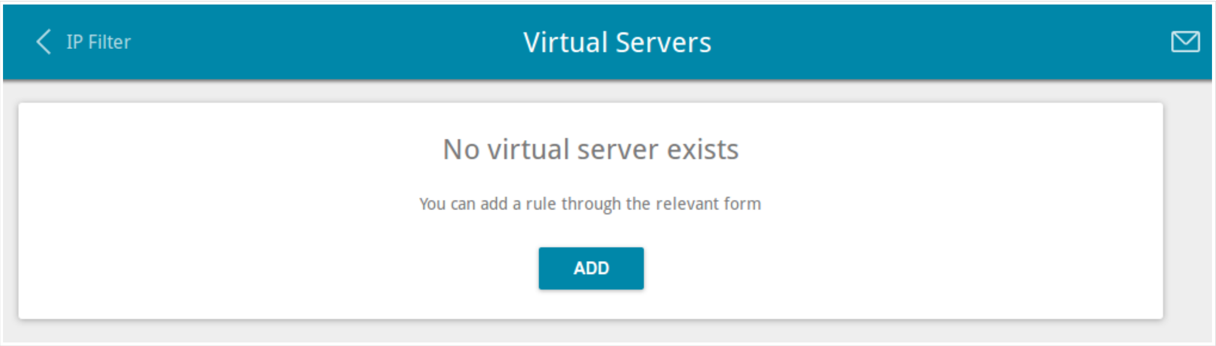
Click the **APPLY** button.

To edit a rule for IP filtering, select the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

To remove a rule, select the checkbox located to the left of the relevant line of the table and click the **DELETE** button. Also you can remove a rule on the editing page.

Virtual Servers

On the **Firewall / Virtual Servers** page, you can create virtual servers for redirecting incoming Internet traffic to a specified IP address in the local area network.

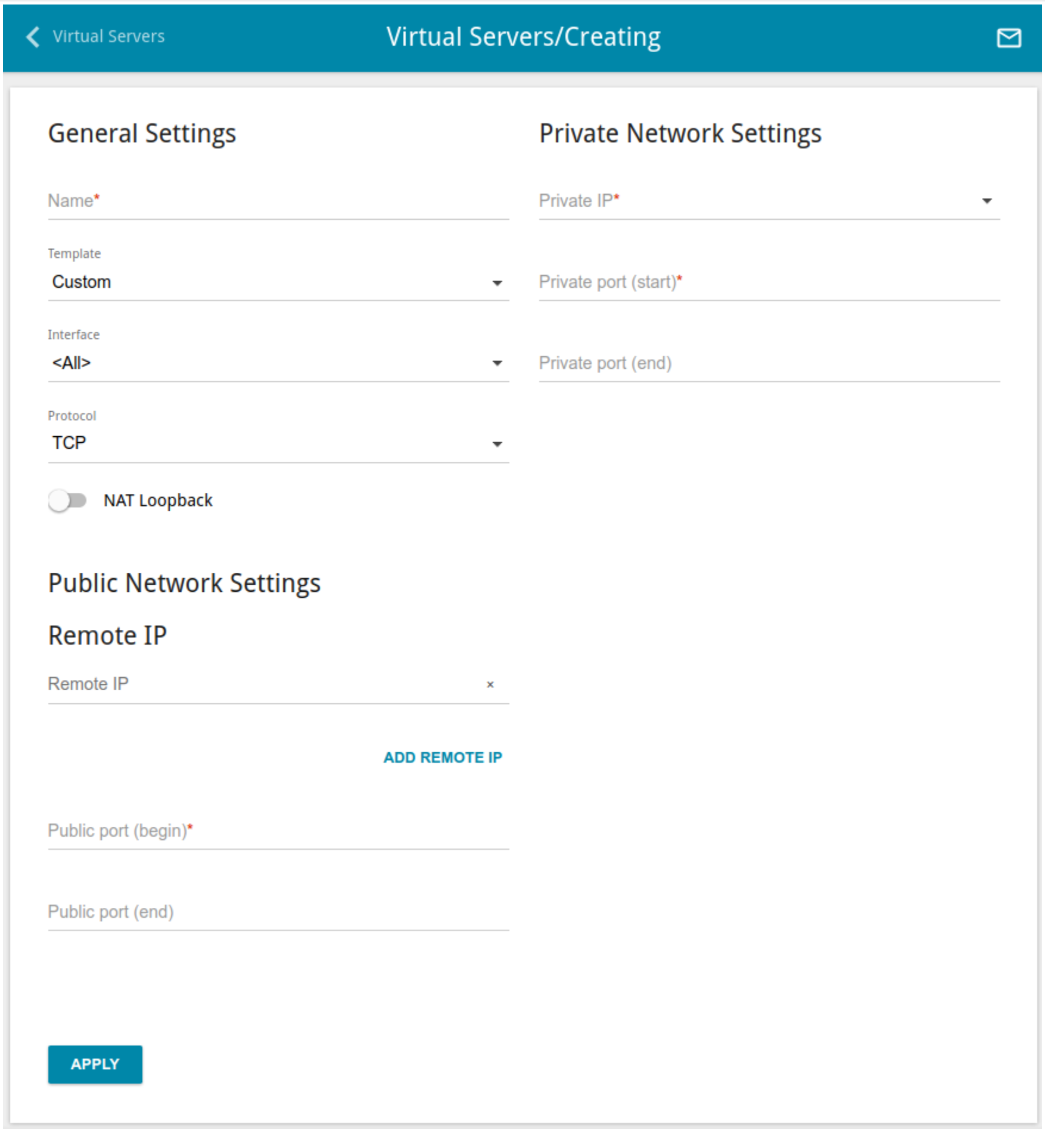


No virtual server exists

You can add a rule through the relevant form

*Figure 153. The **Firewall / Virtual Servers** page.*

To create a new virtual server, click the **ADD** button.



General Settings

Name*

Template: Custom

Interface: <All>

Protocol: TCP

NAT Loopback

Public Network Settings

Remote IP

Remote IP

Public port (begin)*

Public port (end)

Private Network Settings

Private IP*

Private port (start)*

Private port (end)

Figure 154. The page for adding a virtual server.

You can specify the following parameters:

Parameter	Description
General Settings	
Name	A name for the virtual server for easier identification. You can specify any name.
Template	Select a virtual server template from the drop-down list, or select **Custom** to specify all parameters of the new virtual server manually.
Interface	A WAN connection to which this virtual server will be assigned.
Protocol	A protocol that will be used by the new virtual server. Select a value from the drop-down list.
NAT Loopback	Move the switch to the right in order to let the users of the router's LAN access the local server using the external IP address of the router or its DDNS name (if a DDNS service is configured). Users from the external network access the router using the same address (or DDNS name).
Public Network Settings	
Remote IP	Enter the IP address of the server from the external network. To add one more IP address, click the **ADD REMOTE IP** button and enter the address in the displayed line. To remove the IP address, click the **Delete** icon (×) in the line of the address.
Public port (begin)/ Public port (end)	A port of the router from which traffic is directed to the IP address specified in the **Private IP** field in the **Private Network Settings** section. Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the **Public port (begin)** field and leave the **Public port (end)** field blank.
Private Network Settings	
Private IP	The IP address of the server from the local area network. To choose a device connected to the router's LAN at the moment, select the relevant value from the drop-down list (the field will be filled in automatically).

Parameter	Description
Private port (start)/ Private port (end)	A port of the IP address specified in the **Private IP** field to which traffic is directed from the **Public port**. Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the **Private port (start)** field and leave the **Private port (end)** field blank.

Click the **APPLY** button.

To edit the parameters of an existing server, select the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

To remove a server, select the checkbox located to the left of the relevant line of the table and click the **DELETE** button. Also you can remove a server on the editing page.

DMZ

A DMZ is a host or network segment located “between” internal (local) and external (global) networks. In the router, the DMZ implements the capability to transfer a request coming to a port of the router from the external network to a specified host of the internal network.

On the **Firewall / DMZ** page, you can specify the IP address of the DMZ host.

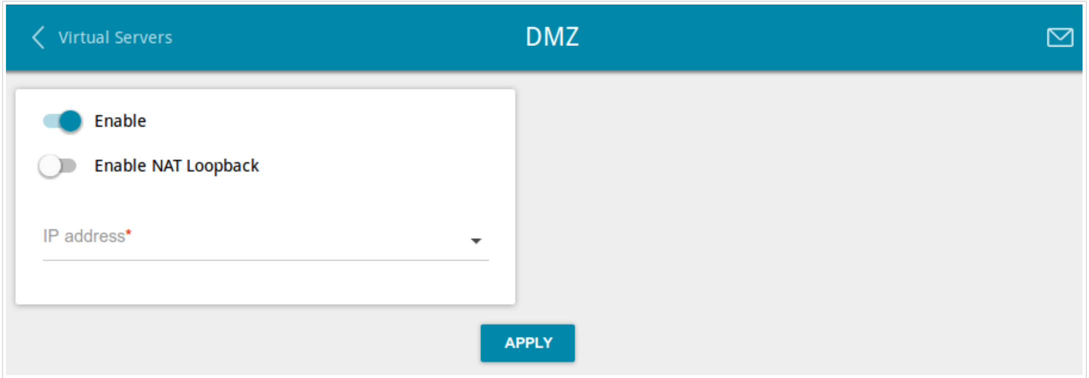


*Figure 155. The **Firewall / DMZ** page.*

To enable the DMZ, move the **Enable** switch to the right.

Enter the IP address of a host from your network in the **IP address** field. To choose a device connected to the router's LAN at the moment, select the relevant value from the drop-down list (the field will be filled in automatically).

Move the **Enable NAT Loopback** switch to the right in order to let the users of the router's LAN access the DMZ host using the external IP address of the router or its DDNS name (if a DDNS service is configured). Users from the external network access the router using the same address (or DDNS name).

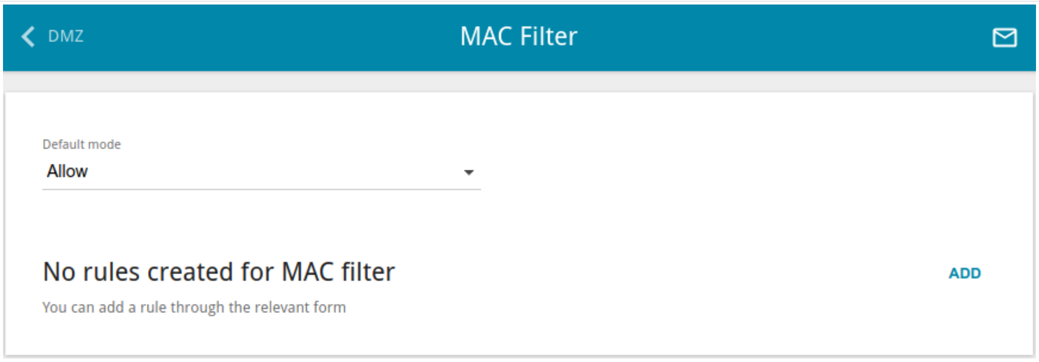
Click the **APPLY** button.

Note that when the DMZ is enabled, all traffic coming to a port of the WAN interface of the router is directed to the same port of the specified IP address. Also note that virtual servers have higher priority than the DMZ host. In other words, if there has been created a virtual server that directs traffic from external port 80 to a port of the device from the router's local network, then entering `http://router_WAN_IP` in the address bar, users of the external network are directed to the specified port and IP address configured for the virtual server, but not to port 80 of the device with the IP address specified on the **Firewall / DMZ** page.

To disable the DMZ, move the **Enable** switch to the left and click the **APPLY** button.

MAC Filter

On the **Firewall / MAC Filter** page, you can configure MAC-address-based filtering for computers of the router's LAN.



Default mode
Allow

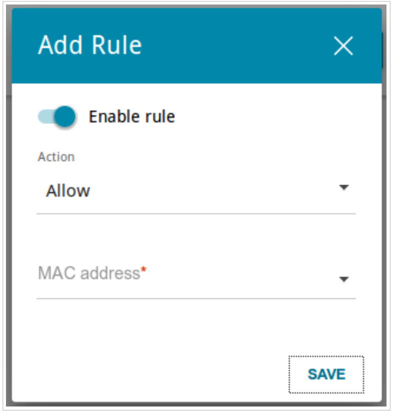
No rules created for MAC filter
You can add a rule through the relevant form

*Figure 156. The **Firewall / MAC Filter** page.*

Select the needed action from the drop-down list in the **Default mode** section to configure filtering for all devices of the router's network:

- **Allow**: Allows access to the router's network and to the Internet for devices (the value is specified by default);
- **Deny**: Blocks access to the router's network for devices.

If you need to specify a filtering mode for each device separately, create a relevant rule. To do this, click the **ADD** button.



Enable rule

Action
Allow

MAC address*

Figure 157. The window for adding a rule for the MAC filter.

In the opened window, you can specify the following parameters:

Parameter	Description
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Action	Select an action for the rule. **Deny**: Blocks access to the router's network for the device with the specified MAC address. **Allow**: Allows access to the router's network and to the Internet for the device with the specified MAC address when the rules on the **Firewall / IP Filter** page block access for this device.
MAC address	The MAC address of a device from the router's LAN. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).

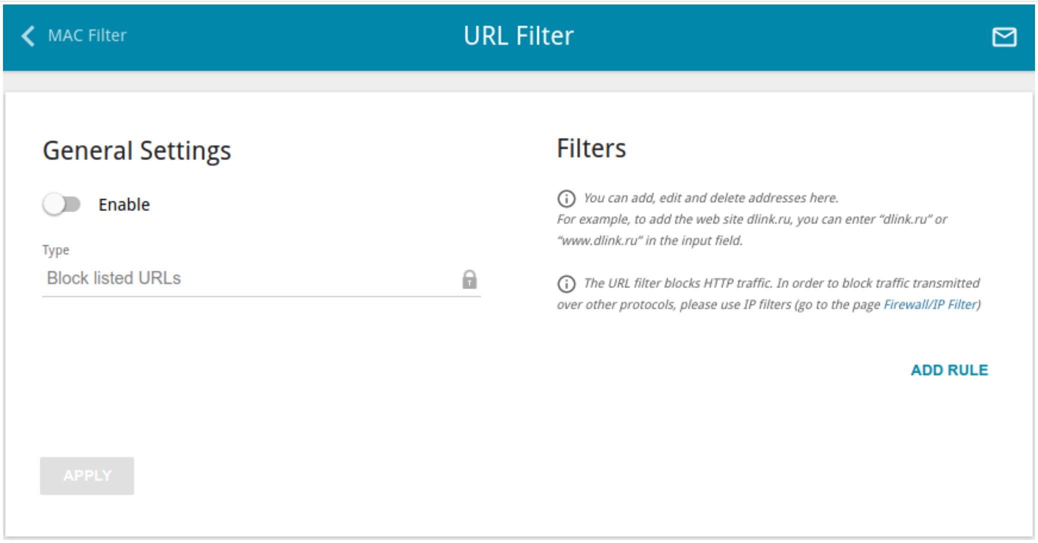
After specifying the needed parameters, click the **SAVE** button.

To edit a rule, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a rule, select the checkbox located to the left of the relevant line of the table and click the **DELETE** button. Also you can remove a rule in the editing window.

URL Filter

On the **Firewall / URL Filter** page, you can specify restrictions on access to certain web sites.



Type: Block listed URLs

You can add, edit and delete addresses here.
For example, to add the web site dlink.ru, you can enter "dlink.ru" or "www.dlink.ru" in the input field.

The URL filter blocks HTTP traffic. In order to block traffic transmitted over other protocols, please use IP filters (go to the page Firewall/IP Filter)

*Figure 158. The **Firewall / URL Filter** page.*

To enable the URL filter, in the **General Settings** section, move the **Enable** switch to the right, then select the needed mode from the **Type** drop-down list:

- **Block listed URLs**: when this value is selected, the router blocks access to all addresses specified in the **Filters** section;
- **Block all URLs except listed**: when this value is selected, the router allows access to addresses specified in the **Filters** section and blocks access to all other web sites.

Click the **APPLY** button.

To specify URL addresses to which the selected filtering mode will be applied, in the **Filters** section, click the **ADD RULE** button and enter a relevant address in the displayed line. Then click the **APPLY** button.

To remove an address from the list of URL addresses, click the **Delete** icon (×) in the line of the relevant URL address. Then click the **APPLY** button.

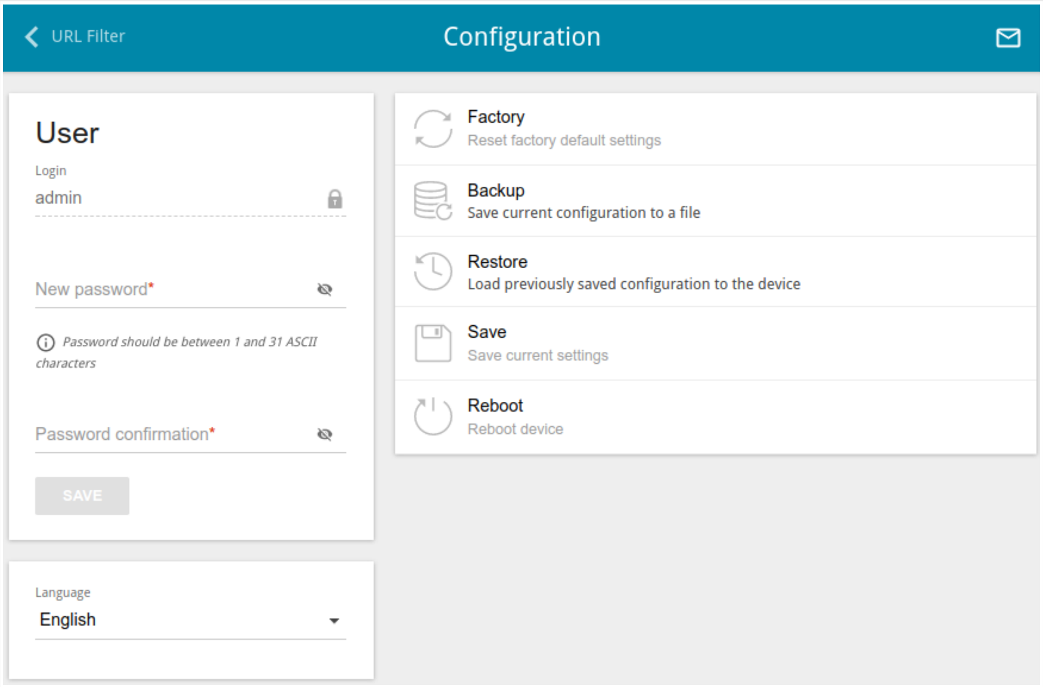
System

In this menu you can do the following:

- change the password used to access the router's settings
- restore the factory default settings
- create a backup of the router's configuration
- restore the router's configuration from a previously saved file
- save the current settings to the non-volatile memory
- reboot the router
- change the web-based interface language
- update the firmware of the router
- configure automatic notification on new firmware version
- view the system log; configure sending the system log to a remote host and/or a USB storage connected to the router
- check availability of a host on the Internet through the web-based interface of the router
- trace the route to a host
- allow or forbid access to the router via TELNET
- configure automatic synchronization of the system time or manually configure the date and time for the router.

Configuration

On the **System / Configuration** page, you can change the password for the administrator account used to access the web-based interface of the router and to access the device settings via TELNET, restore the factory defaults, backup the current configuration, restore the router's configuration from a previously created file, save the changed settings to the non-volatile memory, reboot the device, or change the web-based interface language.



User
Login
admin
New password*
Password should be between 1 and 31 ASCII characters
Password confirmation*

Language
English

Factory
Reset factory default settings

Backup
Save current configuration to a file

Restore
Load previously saved configuration to the device

Save
Save current settings

Reboot
Reboot device

*Figure 159. The **System / Configuration** page.*

In order to change the password for the administrator account, in the **User** section, enter a new password in the **New password** and **Password confirmation** fields. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[16] Click the **Show** icon (👁) to display the entered values. Then click the **SAVE** button.

! Remember or write down the new password for the administrator account. In case of losing the new password, you can access the settings of the router only after restoring the factory default settings via the hardware **RESET** button. This procedure wipes out all settings that you have configured for your router.

To change the web-based interface language, select the needed value from the **Language** drop-down list.

[16] 0-9, A-Z, a-z, space, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

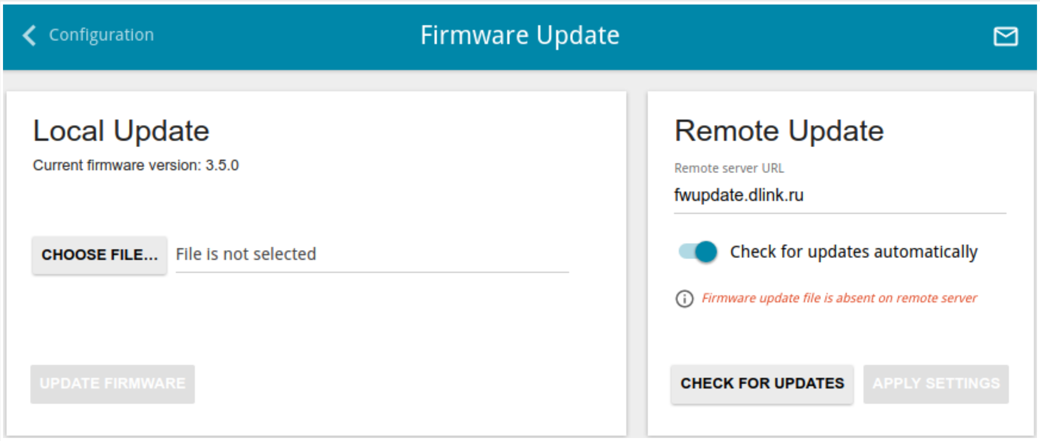
The following buttons are also available on the page:

Control	Description
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware **RESET** button (see the ***Back Panel*** section, page 16).
Backup	Click the button to save the configuration (all settings of the router) to your PC. The configuration backup will be stored in the download location of your web browser.
Restore	Click the button and follow the dialog box appeared to select a previously saved configuration file (all settings of the router) located on your PC and upload it.
Save	Click the button to save settings to the non-volatile memory. The router saves changed settings automatically. If changed settings have not been saved automatically, a notification is displayed in the top right part of the page.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

Firmware Update

On the **System / Firmware Update** page, you can update the firmware of the router and configure the automatic check for updates of the router's firmware.

! Update the firmware only when the router is connected to your PC via a wired connection.



Current firmware version: 3.5.0

File is not selected

Remote server URL
fwupdate.dlink.ru

Check for updates automatically

Firmware update file is absent on remote server

*Figure 160. The **System / Firmware Update** page.*

The current version of the router's firmware is displayed in the **Current firmware version** field.

By default, the automatic check for the router's firmware updates is enabled. If a firmware update is available, a notification will be displayed in the top right corner of the page.

To disable the automatic check for firmware updates, in the **Remote update** section, move the **Check for updates automatically** switch to the left and click the **APPLY SETTINGS** button.

To enable the automatic check for firmware updates, in the **Remote update** section, move the **Check for updates automatically** switch to the right and click the **APPLY SETTINGS** button.

By default, in the **Remote server URL** field, the D-Link update server address (**`fwupdate.dlink.ru`**) is specified.

You can update the firmware of the router locally (from the hard drive of your PC) or remotely (from the update server).

Local Update

! Attention! Do not turn off the router before the firmware update is completed. This may cause the device breakdown.

To update the firmware of the router locally, follow the next steps:

1. Download a new version of the firmware from www.dlink.ru.
2. Click the **CHOOSE FILE** button in the **Local Update** section on the **System / Firmware Update** page to locate the new firmware file.
3. Click the **UPDATE FIRMWARE** button.
4. Wait until the router is rebooted (about one and a half or two minutes).
5. Log into the web-based interface using the login (**admin**) and the current password.

If after updating the firmware the router doesn't work correctly, please restore the factory default settings. To do this, click the **Factory** button on the **System / Configuration** page. Wait until the router is rebooted.

Remote Update

! Attention! Do not turn off the router before the firmware update is completed. This may cause the device breakdown.

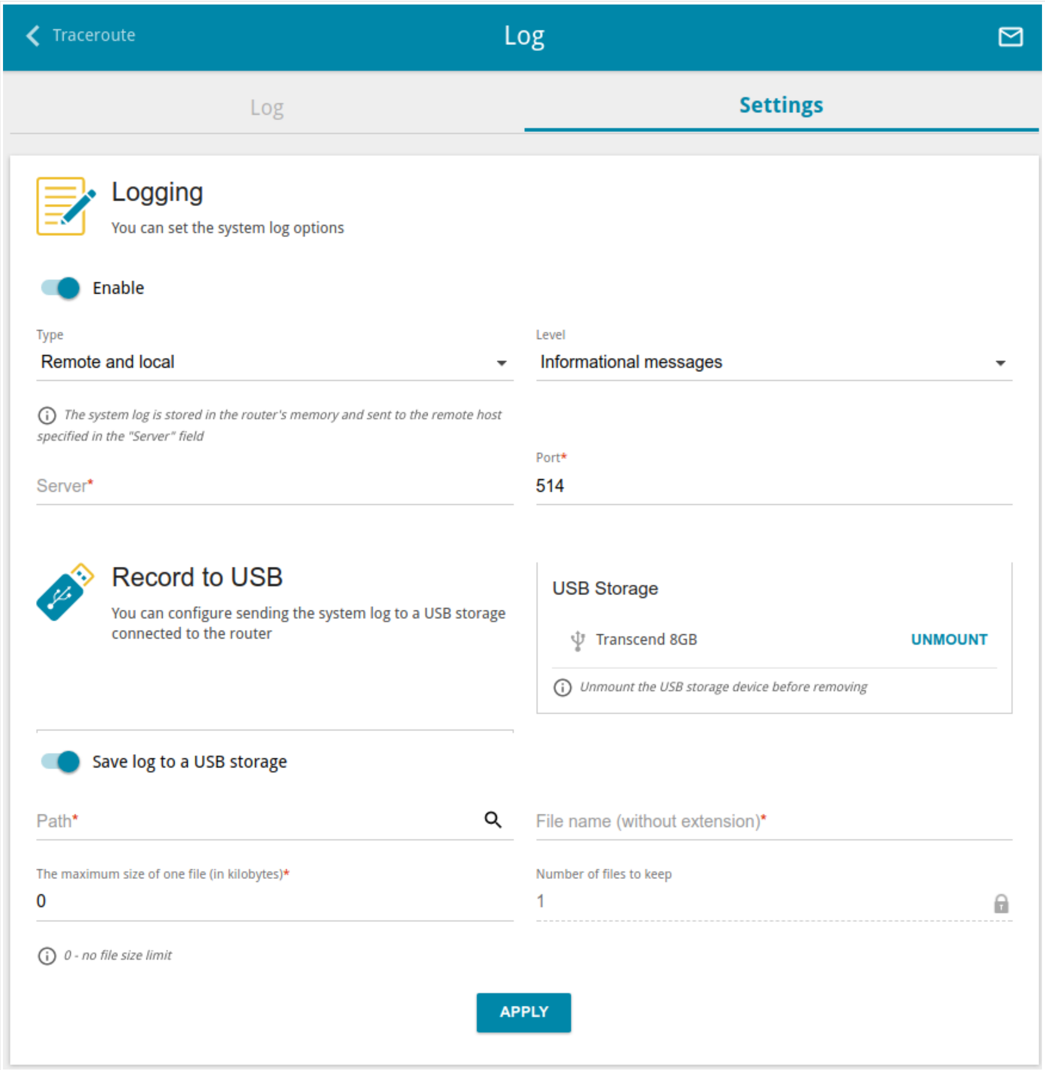
To update the firmware of the router remotely, follow the next steps:

1. On the **System / Firmware Update** page, in the **Remote Update** section, click the **CHECK FOR UPDATES** button to check if a newer firmware version exists.
2. Click the **UPDATE FIRMWARE** button (the button is displayed if a newer version of the firmware is available).
3. Wait until the router is rebooted (about one and a half or two minutes).
4. Log into the web-based interface using the login (`admin`) and the current password.

If after updating the firmware the router doesn't work correctly, please restore the factory default settings. To do this, click the **Factory** button on the **System / Configuration** page. Wait until the router is rebooted.

Log

On the **System / Log** page, you can set the system log options and configure sending the system log to a remote host and/or a USB storage connected to the router.



Logging
You can set the system log options

Enable

Type: Remote and local

Level: Informational messages

The system log is stored in the router's memory and sent to the remote host specified in the "Server" field

Server*

Port*: 514

Record to USB
You can configure sending the system log to a USB storage connected to the router

USB Storage
Transcend 8GB UNMOUNT
Unmount the USB storage device before removing

Save log to a USB storage

Path*

File name (without extension)*

The maximum size of one file (in kilobytes)*: 0

Number of files to keep: 1

0 - no file size limit

APPLY

*Figure 161. The **System / Log** page. The **Settings** tab.*

To enable logging of the system events, go to the **Settings** tab and move the **Enable** switch to the right. Then specify the needed parameters.

Parameter	Description
Logging	
Type	Select a type of logging from the drop-down list. • **Local**: the system log is stored in the router's memory. When this value is selected, the **Server** and **Port** fields are not displayed. • **Remote**: the system log is sent to the remote host specified in the **Server** field. • **Local and remote**: the system log is stored in the router's memory and sent to the remote host specified in the **Server** field.
Level	Select a type of messages and alerts/notifications to be logged.
Server	The IP or URL address of the host from the local or global network, to which the system log will be sent.
Port	A port of the host specified in the **Server** field. By default, the value `514` is specified.
Record to USB	
USB Storage	If a USB storage is connected to the router, its name is displayed in the field. To safely disconnect the USB storage, click the **UNMOUNT** button.
Save log to a USB storage	Move the switch to the right so that the device could send the system log to the USB storage connected to it. Upon that the **Path**, **The maximum size of one file**, **File name**, and **Number of files to keep** fields are displayed.
Path	Click the **Search** icon (🔍) located to the right of the field in order to locate the folder where system log files will be stored.
The maximum size of one file	The maximum size (in kilobytes) of one system log file.
File name	A name for system log files.
Number of files to keep	The maximum number of files allowed to be recorded on the USB storage. When this number is exceeded, the file containing the oldest data will be deleted. The field is available for editing if the value specified in the **The maximum size of one file** field is greater than zero.

After specifying the needed parameters, click the **APPLY** button.

To disable logging of the system events, move the **Enable** switch to the left and click the **APPLY** button.

To view the system log, go to the **Log** tab.

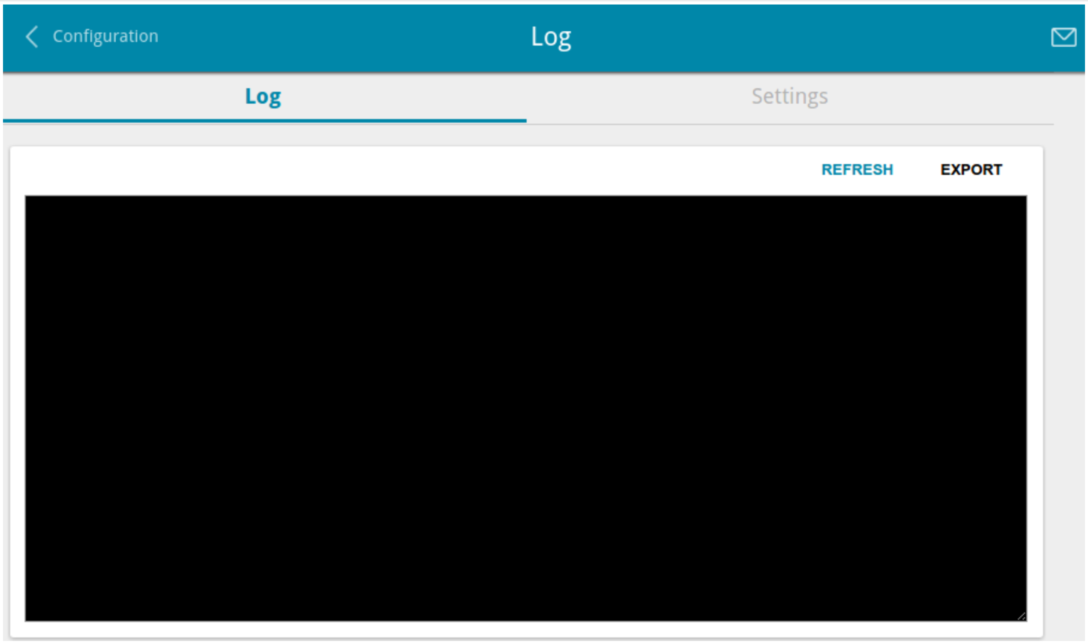


*Figure 162. The **System / Log** page. The **Log** tab.*

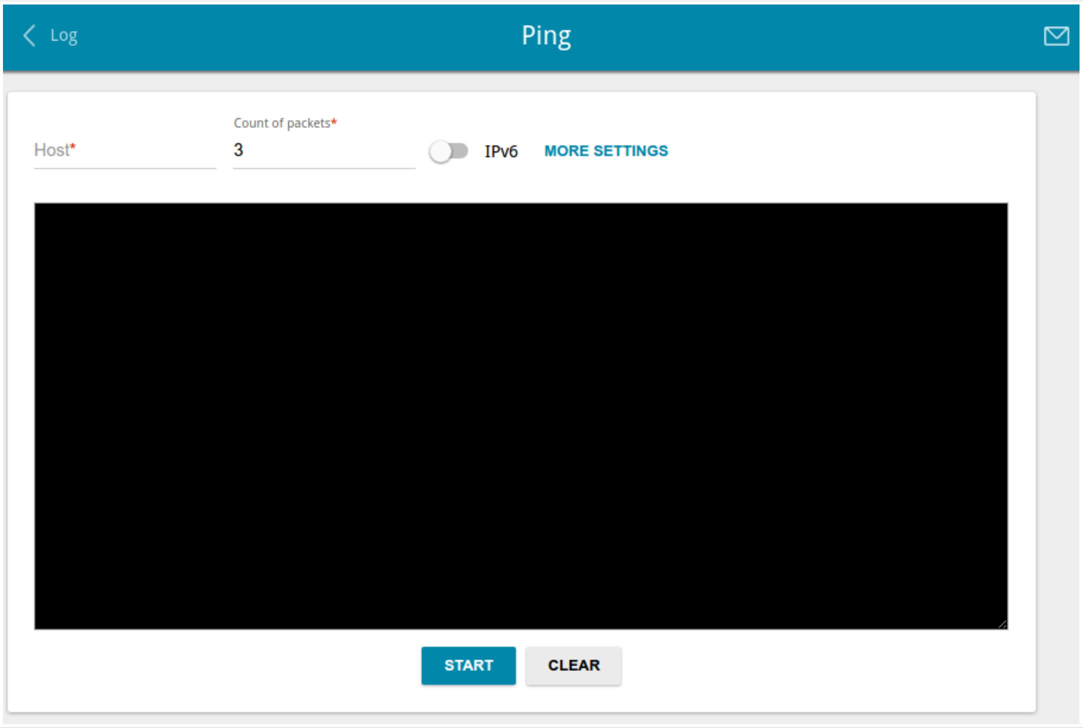
To view the latest system events, click the **REFRESH** button.

To save the system log to your PC, click the **EXPORT** button. The file will be stored in the download location of your web browser.

Ping

On the **System / Ping** page, you can check availability of a host from the local or global network via the Ping utility.

The Ping utility sends echo requests to a specified host and receives echo replies.



Host*

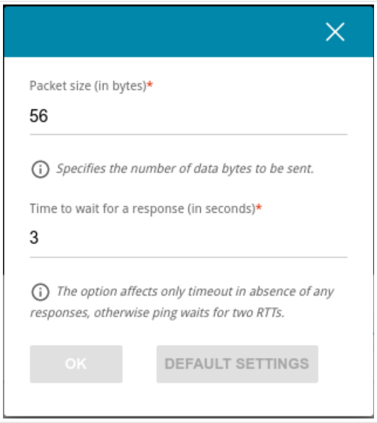
Count of packets*
3

IPv6

*Figure 163. The **System / Ping** page.*

To check availability of a host, enter the IP address or name of this host in the **Host** field and specify a number of requests that will be sent in order to check its availability in the **Count of packets** field. If availability check should be performed with IPv6, move the **IPv6** switch to the right.

To specify additional settings, click the **MORE SETTINGS** button.



Packet size (in bytes)*
56

Specifies the number of data bytes to be sent.

Time to wait for a response (in seconds)*
3

The option affects only timeout in absence of any responses, otherwise ping waits for two RTTs.

*Figure 164. The **System / Ping** page. The additional settings window.*

In the opened window, in the **Packet size** field, specify the volume of data sent in a request. In the **Time to wait for a response** field, specify the response waiting period in seconds. To restore the default field values, click the **DEFAULT SETTINGS** button.

After specifying the additional parameters, click the **OK** button.

To run the check, click the **START** button. After a while, the results will be displayed on the page.

To remove the check result from the page, click the **CLEAR** button.

Traceroute

On the **System / Traceroute** page, you can determine the route of data transfer to a host via the traceroute utility.

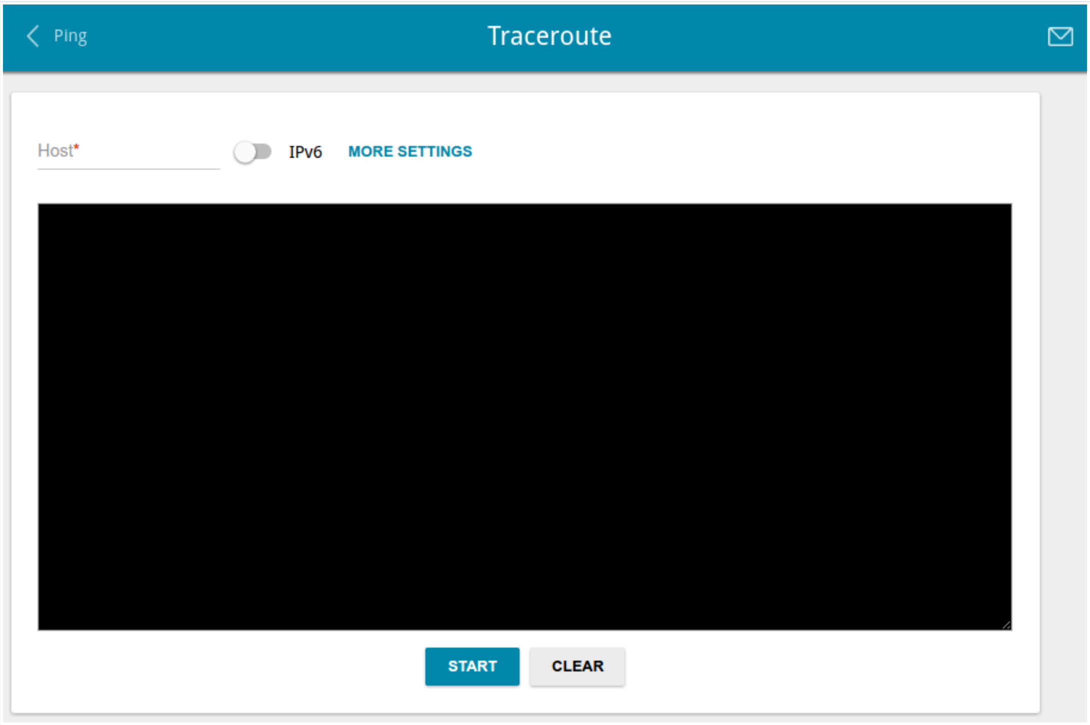
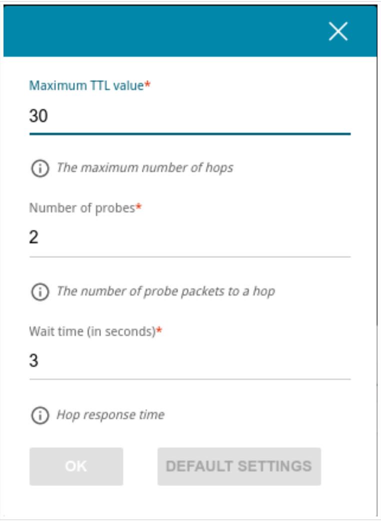


*Figure 165. The **System / Traceroute** page.*

To determine the route, enter the name or IP address of a host in the **Host** field. If the route should be determined using IPv6, move the **IPv6** switch to the right.

To specify additional settings, click the **MORE SETTINGS** button.



Maximum TTL value*: 30
The maximum number of hops

Number of probes*: 2
The number of probe packets to a hop

Wait time (in seconds)*: 3
Hop response time

*Figure 166. The **System / Traceroute** page. The additional settings window.*

In the opened window, you can specify the following parameters:

Parameter	Description
Maximum TTL value	Specify the TTL (*Time to live*) parameter value. The default value is `30`.
Number of probes	The number of attempts to hit an intermediate host.
Wait time	A period of waiting for an intermediate host response.

To restore the default field values, click the **DEFAULT SETTINGS** button.

After specifying the additional parameters, click the **OK** button.

To run the check, click the **START** button. After a while, the results will be displayed on the page. The additional settings window.

To remove the check result from the page, click the **CLEAR** button.

Telnet

On the **System / Telnet** page, you can enable or disable access to the device settings via TELNET from your LAN. Access via TELNET is disabled by default. It is automatically enabled after changing the default administrator password.

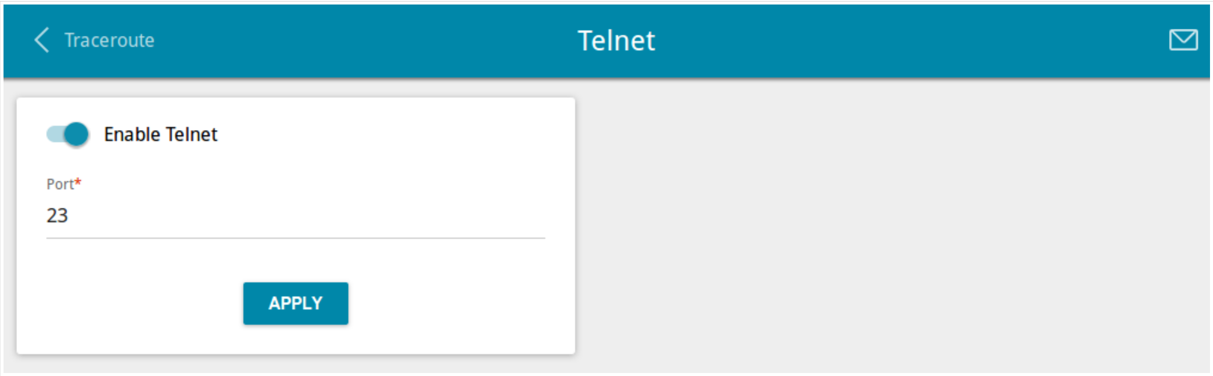


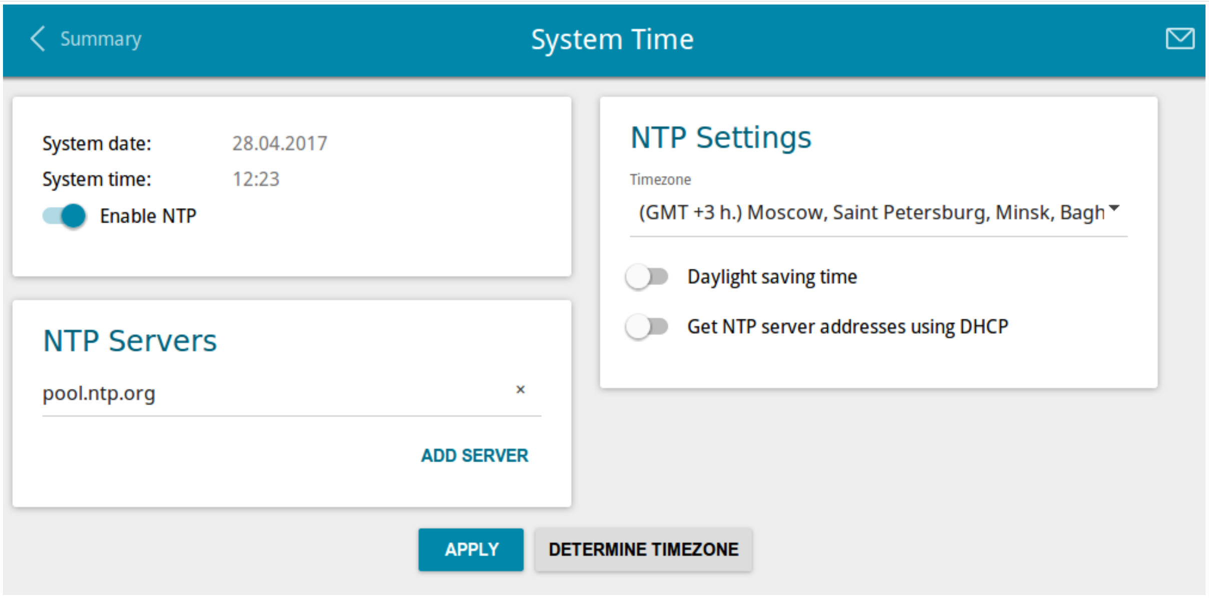
*Figure 167. The **System / Telnet** page.*

To disable access via TELNET, move the **Enable Telnet** switch to the left and click the **APPLY** button.

To enable access via TELNET again, move the **Enable Telnet** switch to the right. In the **Port** field, enter the number of the router's port through which access will be allowed (by default, the port **23** is specified). Then click the **APPLY** button.

System Time

On the **System / System Time** page, you can manually set the time and date of the router or configure automatic synchronization of the system time with a time server on the Internet.



System date: 28.04.2017

System time: 12:23

● Enable NTP

NTP Settings

Timezone: (GMT +3 h.) Moscow, Saint Petersburg, Minsk, Bagh

○ Daylight saving time

○ Get NTP server addresses using DHCP

NTP Servers

pool.ntp.org

*Figure 168. The **System / System Time** page.*

To set the system time manually, follow the next steps:

1. Move the **Enable NTP** switch to the left.
2. In the **Time Settings** section, specify needed values. To specify the time set up your PC or portable device, click the **SET LOCAL TIME** button.
3. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

To enable automatic synchronization with a time server, follow the next steps:

1. Move the **Enable NTP** switch to the right.
2. Specify the needed NTP server or leave the value specified by default in the **NTP Servers** section. If you need to specify several servers, click the **ADD SERVER** button.
3. Select your time zone from the **Timezone** drop-down list in the **NTP Settings** section. To set the time zone in accordance with the settings of your operating system or portable device, click the **DETERMINE TIMEZONE** button.
4. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

To enable automatic adjustment for daylight saving time of the router, move the **Daylight saving time** switch to the right in the **NTP Settings** section and click the **APPLY** button.

In some cases NTP servers addresses are provided by your ISP. In this case, you need to move the **Get NTP server addresses using DHCP** switch in the **NTP Settings** section to the right and click the **APPLY** button. Contact your ISP to clarify if this setting needs to be enabled. If the **Get NTP server addresses using DHCP** switch is moved to the right, the **NTP Servers** section is not displayed.

!

When the router is powered off or rebooted, the system time is reset to the default value. If you have set automatic synchronization for the system time, the internal clock of the device will be configured after connecting to the Internet. If you have set the system time manually, you need to set the time and date again (see above).

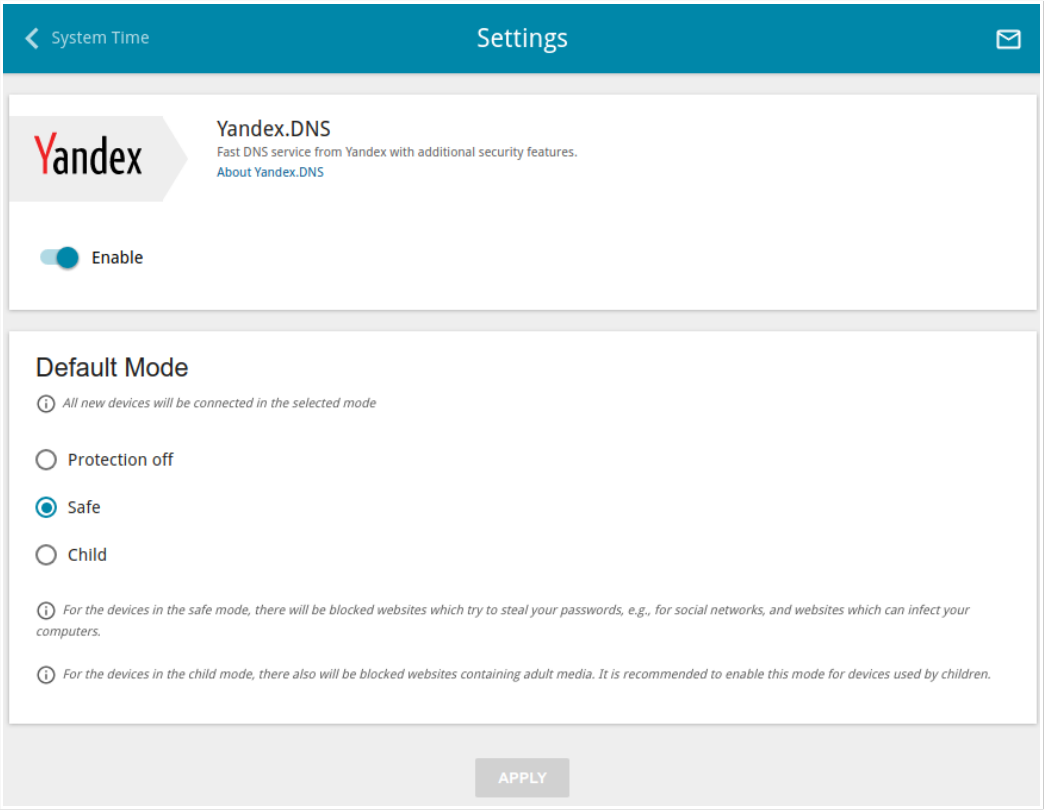
Yandex.DNS

This menu is designed to configure the Yandex.DNS service.

Yandex.DNS is a web content filtering service which provides the DNS server, protects a computer against malicious web sites, and blocks access to adult web sites.

Settings

On the **Yandex.DNS / Settings** page, you can enable the Yandex.DNS service and configure its operating mode.



Yandex.DNS
Fast DNS service from Yandex with additional security features.
About Yandex.DNS

Enable

Default Mode

All new devices will be connected in the selected mode

○ Protection off
● Safe
○ Child

For the devices in the safe mode, there will be blocked websites which try to steal your passwords, e.g., for social networks, and websites which can infect your computers.

For the devices in the child mode, there also will be blocked websites containing adult media. It is recommended to enable this mode for devices used by children.

*Figure 169. The **Yandex.DNS / Settings** page.*

To get detailed information on the service, click the **About Yandex.DNS** link.

To enable the Yandex.DNS service, move the **Enable** switch to the right.

When the service is enabled, the **Default Mode** section is displayed on the page. Select the needed choice of the radio button to configure filtering for all devices of the router's network:

- **Protection off**: when this value is selected, the service provides the DNS server with no restrictions on access to unsafe web sites;
- **Safe**: when this value is selected, the service blocks access to malicious and fraudulent web sites;
- **Child**: when this value is selected, the service blocks access to malicious and fraudulent web sites and blocks access to adult content.

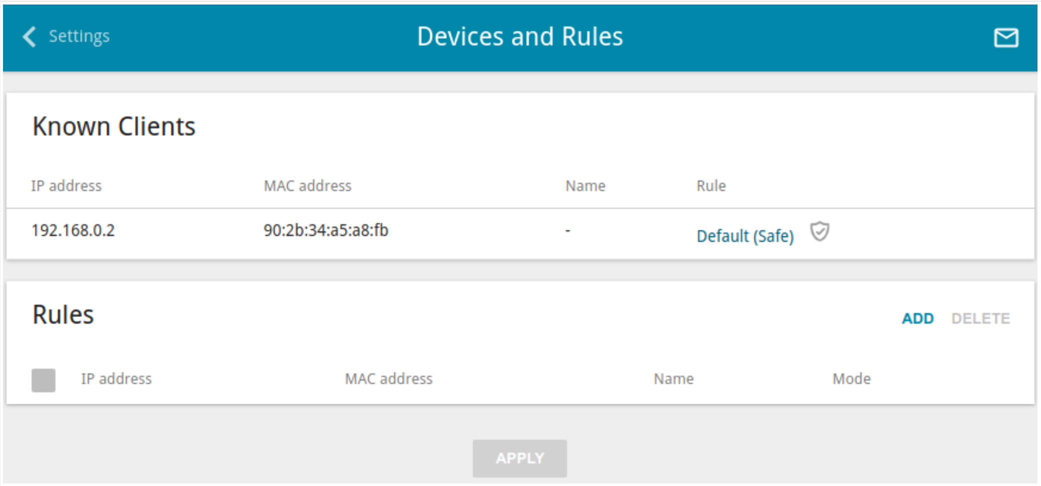
Also the selected filtering mode will be applied to all devices newly connected to the router's network.

After specifying all needed parameters, click the **APPLY** button.

To disable the Yandex.DNS service, move the **Enable** switch to the left and click the **APPLY** button.

Devices and Rules

On the **Yandex.DNS / Devices and Rules** page, you can specify a filtering mode for each device separately.



< Settings — Devices and Rules

Known Clients

IP address	MAC address	Name	Rule
192.168.0.2	90:2b:34:a5:a8:fb	-	Default (Safe)

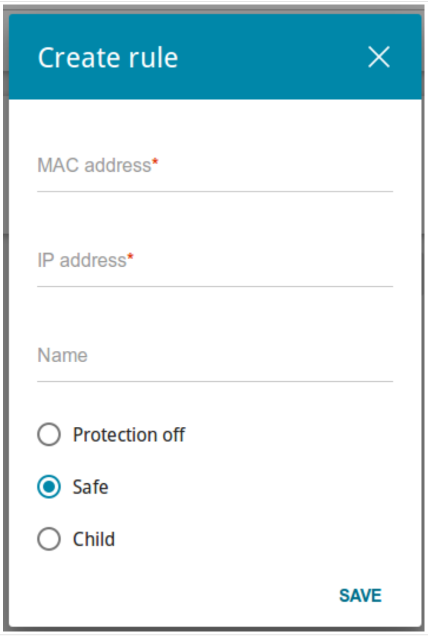
Rules — ADD DELETE

□	IP address	MAC address	Name	Mode

*Figure 170. The **Yandex.DNS / Devices and Rules** page.*

In the **Known Clients** section, the devices connected to the local network of the router at the moment and their relevant filtering mode are displayed.

To create[17] a new filtering rule for a device, click the **ADD** button in the **Rules** section, or left-click the name of the filtering mode in the line of the device for which a rule should be created in the **Known Clients** section.



Create rule

MAC address*

IP address*

Name

○ Protection off
● Safe
○ Child

Figure 171. Adding a new rule for the Yandex.DNS service.

[17] When a new rule for filtering is created, a MAC address and IP address pair is displayed on the **Connections Setup / LAN** page. The created pair will be deleted with the relevant rule.

In the opened window, you can specify the following parameters:

Parameter	Description
MAC address	The MAC address of a device from the router's LAN.
IP address	The IP address of a device from the router's LAN.
Name	Enter a name for the rule for easier identification. *Optional*.
Mode	Select an operating mode of the Yandex.DNS service for this rule. **Protection off**: when this value is selected, the service provides the DNS server with no restrictions on access to unsafe web sites. **Safe**: when this value is selected, the service blocks access to malicious and fraudulent web sites. **Child**: when this value is selected, the service blocks access to malicious and fraudulent web sites and blocks access to adult content.

After specifying the needed parameters, click the **SAVE** button.

To edit a rule for filtering, select a relevant line of the table, in the opened window, change the needed values and click the **SAVE** button.

To remove a rule for filtering, select the checkbox located to the left of the relevant rule and click the **DELETE** button. Also you can remove a rule in the editing window.

After completing the work with rules, click the **APPLY** button.

CHAPTER 5. OPERATION GUIDELINES

Safety Rules and Conditions

Please carefully read this section before installation and connection of the device. Make sure that the power adapter and cables are not damaged. The device should be used only as intended in accordance with the documents.

The device is intended for use in dry, clean, dust-free, and well ventilated areas with normal humidity away from strong heat sources. Do not use the device outdoors or in the areas with high humidity. Do not place foreign objects on the device. Do not obstruct the ventilation openings of the device. The environmental temperature near the device and the temperature inside the device's cover should be within the range from 0 °C to +40 °C.

Only use the power adapter supplied with the device. Do not plug in the adapter, if its case or cable are damaged. Plug the adapter only into working electrical outlets with parameters indicated on the adapter.

Do not open the cover of the device! Unplug the device before dusting and cleaning. Use a damp cloth to clean the device. Do not use liquid/aerosol cleaners or magnetic/static cleaning devices. Prevent moisture getting into the device or the power adapter.

The service life of the device is 2 years.

Wireless Installation Considerations

The DIR-853 device lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF noise in your home or office. To maximize your wireless range, follow the guidelines below.

1. Keep the number of walls and ceilings between the DIR-853 device and other network devices to a minimum – each wall or ceiling can reduce your wireless network range by 3-90 feet (1-30 meters).
2. Be aware of the direct line between network devices. Place your devices so that the signal travels straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on your wireless range. Try to position your router, access points, and computers so that the signal passes through drywalls or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your router away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 equipment (wireless devices such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. Note, that the base transmits a signal even if the phone in not in use.

CHAPTER 6. ABBREVIATIONS AND ACRONYMS

3G	Third Generation
AC	Access Category
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BSSID	Basic Service Set Identifier
CRC	Cyclic Redundancy Check
DDNS	Dynamic Domain Name System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTIM	Delivery Traffic Indication Message
GMT	Greenwich Mean Time
GSM	Global System for Mobile Communications
IGD	Internet Gateway Device
IGMP	Internet Group Management Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LTE	Long Term Evolution
MAC	Media Access Control
MTU	Maximum Transmission Unit

NAT	Network Address Translation
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
PBC	Push Button Configuration
PIN	Personal Identification Number
PPPoE	Point-to-point protocol over Ethernet
PPTP	Point-to-point tunneling protocol
PSK	Pre-shared key
PUK	PIN Unlock Key
QoS	Quality of Service
RADIUS	Remote Authentication in Dial-In User Service
RIP	Routing Information Protocol
RTS	Request To Send
RTSP	Real Time Streaming Protocol
SIP	Session Initiation Protocol
SIM	Subscriber Identification Module
SMB	Server Message Block
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity

WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup